AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT AND CRIMINAL COMPLAINT AND ARREST WARRANT

I, Cory P. McManus, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I make this affidavit in support of an application for a criminal complaint charging:

   a. Patrick JOHNSON (YOB 1984) with Wire Fraud in violation of 18 U.S.C. § 1343, Bank Fraud in violation of 18 U.S.C. § 1344, Conspiracy to Commit Wire Fraud and Bank Fraud in violation of 18 U.S.C. § 1349, and Aggravated Identity Theft in violation of 18 U.S.C. § 1028A.

   b. Terrance RICHARDSON (YOB 1991) with Bank Fraud in violation of 18 U.S.C. § 1344, Wire Fraud in violation of 18 U.S.C. § 1343, Conspiracy to Commit Wire and Bank Fraud in violation of 18 U.S.C. § 1349, and Aggravated Identity Theft in violation of 18 U.S.C. § 1028A.

   c. Richard KOBOI (YOB 1995) with Bank Fraud in violation of 18 U.S.C. § 1344, Wire Fraud in violation of 18 U.S.C. § 1343, Conspiracy to Commit Wire and Bank Fraud in violation of 18 U.S.C. § 1349, and Aggravated Identity Theft in violation of 18 U.S.C. § 1028A.

2. I also make this affidavit under Rule 41 of the Federal Rules of Criminal Procedure in support of an application for search warrants for the search of the following premises, cellphones and digital storage devices, and vehicle:

   a. 211 Hanover Street, Apt 1, Providence, RI (hereinafter referred to as "SUBJECT PREMISES 1"), and any safes, lockers and closed containers therein and any outbuildings associated with 211 Hanover Street, Providence, RI, as more particularly described in Attachment A-1 (attached hereto and incorporated herein by reference), including any person present at the time the search warrant is executed, for the items described in Attachment B-1.

   b. 439 Admiral St, Apt 3, Providence, RI (hereinafter referred to as "SUBJECT PREMISES 2"), and any safes, lockers and closed containers therein and any outbuildings associated with 439 Admiral St, Apt 3, Providence, RI , as more particularly described in Attachment A-2 (attached hereto and incorporated herein by reference),

including any person present at the time the search warrant is executed, for the items described in Attachment B-2.

c. 91 Hartford Ave., Apt 131, Providence, RI (hereinafter referred to as "SUBJECT PREMISES 3"), and any safes, lockers and closed containers therein and any outbuildings associated with 91 Hartford Ave., Apt 131, Providence, RI, as more particularly described in Attachment A-3 (attached hereto and incorporated herein by reference), including any person present at the time the search warrant is executed, for the items described in Attachment B-3.

d. The cellular telephone associated with telephone number (401) 677-9165 (TARGET PHONE #1), currently anticipated to be in the possession of Terrance RICHARDSON, and any cellular telephones or digital storage devices he may have on his person, and the extraction from that property of electronically stored information described in Attachment B-2.

e. The cellular telephone associated with telephone number (267) 854-9972 (TARGET PHONE #2), currently anticipated to be in the possession of Richard KOBOI, and any cellular telephones or digital storage devices he may have on his person, and the extraction from that property of electronically stored information described in Attachment B-3;

f. The cellular telephone associated with telephone number (401) 648-5717 (TARGET PHONE #3), currently anticipated to be in the possession of Patricia JOHNSON, and any cellular telephones or digital storage devices she may have on her person, and the extraction from that property of electronically stored information described in Attachment B-1.

g. A silver Chevrolet Colorado bearing CA registration 37035X2 (TARGET VEHICLE) registered to Hertz Vehicles, LLC out of Los Angeles, CA, for the items described in Attachment B-3.

I further make this affidavit in support of an application for search warrants under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(l)(A) for:

a. information about the location of the cellular telephone assigned telephone number (401) 677-9165, with International Mobile Subscriber Identity Number 310260270097507 ("TARGET PHONE #1"). The phone service provider for

TARGET PHONE 1 is T-Mobile, a wireless service provider located in Parsippany, New Jersey. The subscriber information is Agretta Richardson, 21 Milk St, Providence, RI 02905 and was activated in July of 2019. TARGET PHONE #1 is described herein and in Attachment C-1, and the location information to be seized is described herein and in Attachment D.

b. information about the location of the cellular telephone assigned telephone number (267) 854-9972, ("TARGET PHONE #2"). The phone service provider for TARGET PHONE #2 is T-Mobile, a wireless service provider located in Parsippany, New Jersey. Due to this phone being a Tracfone[1], there is no subscriber information associated with the phone number. TARGET PHONE #2 is described herein and in Attachment C-2, and the location information to be seized is described herein and in Attachment D.

3. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," see 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. See 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. See 18 U.S.C. § 3123(b)(1).

4. The court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

5. The statements contained in this Affidavit are based on my personal observations, my training and experience, information obtained from other agents, witnesses, and records obtained during the course of the investigation. Because I submit this Affidavit for the limited purpose of showing probable cause, I have not included in this Affidavit each and every fact that I have learned in this investigation. Rather, I have set forth only facts sufficient to establish probable cause to issue an arrest warrant and search warrant for the

[1] Tracfone Wireless is a mobile virtual network operator (MVNO) that provides both prepaid service and variety of branded smartphones to use with their service. They do not have any contracts and all airtime has unlimited carry over for talk, text, and data.

individuals and premises identified herein. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. AFFIANT BACKGROUND

6. I have been a law enforcement officer for over 17 years and have been a United States Postal Inspector since July 2017. I am currently assigned to the Providence, Rhode Island field office of the United States Postal Inspection Service and I am responsible for the investigation of various crimes relating to the United States Mail including, but not limited to mail fraud, bank fraud, identity theft, and mail theft. Prior to my appointment as a Postal Inspector, I was a Special Agent with the United States Secret Service for approximately 13 years. I have received training in conducting investigations of crimes that adversely affect, or fraudulently use, the United States Mail and the United States Postal Service (USPS). I have participated in criminal investigations of various violations of Title 18 of the United States Code involving financial crimes, including mail, bank, and wire fraud, identity theft, money laundering, and computer crimes. In the course of my employment I have received training and have been involved in the use of investigative techniques such as interviewing victims, informants, and witnesses, conducting physical surveillance, and analyzing financial records. I have participated in and executed several search and arrest warrants.

III. PROBABLE CAUSE

7. As set forth in this Affidavit, the U.S. Attorney's Office for the District of Rhode Island, the U.S. Postal Inspection Service (USPIS) and the Federal Bureau of Investigation (FBI) have been investigating a scheme in which the perpetrators mailed out counterfeit Home Equity Line Of Credit (HELOC) checks to individuals throughout the country. From Post Office (PO) surveillance videos, we were able to identify Patrick JOHNSON as the individual mailing counterfeit checks on November 20, 2019, from the Olneyville PO, November 26, 2019, from the Olneyville PO, and December 23, 2019, from the Elmwood PO.

8. In addition to these HELOC counterfeit check mailings to individuals throughout the country, the investigation revealed that Patrick JOHNSON, as well as Terrance RICHARDSON a.k.a. Teebone Juheard, and Richard KOBOI a.k.a. Sunnyboy Taylor were providing counterfeit checks, including those drawn upon businesses, to individuals whose banks accounts they were using to deposit the funds, and/or depositing the checks themselves into the individuals' bank accounts, then causing the funds to be withdrawn. Not only were they using other individuals' bank accounts, bank records for RICHARDSON and KOBOI's bank accounts as well bank surveillance videos also show that they were depositing the counterfeit checks into their own accounts and/or withdrawing these funds.
9. Facebook records associated with RICHARDSON and KOBOI further showed that RICHARDSON and KOBOI solicited individuals with bank account information in this counterfeit check cashing scheme. Patricia JOHNSON, the daughter of Patrick JOHNSON, was one of the individuals whose bank account was used with her assistance to deposit a counterfeit check. In addition, the funds of a separate counterfeit check transaction were used to purchase two postal money order made payable to Patricia JOHNSON's whose driver's license was presented during that transaction.
10. In addition, Terrance RICHARDSON used the name of a real individual on a counterfeit check and the real individual's debit card information to deposit a counterfeit check into that individual's bank account, Richard KOBOI used the name and forged signature of real individual in an attempt to deposit a U.S. Treasury check into KOBOI's own bank account, and Patrick JOHNSON also used the name and identifying information of a real individual in a credit application in an attempt to fraudulently obtain a credit card in the victim's name.

COUNTERFEIT HELOC CHECK MAILINGS

11. A home equity line of credit, also known as a HELOC, is a line of credit secured by your home that gives you a revolving credit line to use for large expenses or to consolidate higher-interest rate debt on other loans such as credit cards. A HELOC often has a lower interest rate than some other common types of loans, and the interest may be tax deductible. Most banks offer a number of different ways to access those funds, whether

it's through an online transfer, writing a check, or using a credit card connected to your account.

12. In January 2020, a Pawtucket Credit Union (CU) Bank investigator notified USPIS Postal Inspector Cory McManus and FBI Special Agent Matt Riportella regarding several Pawtucket CU customers who had their account information compromised. The investigator advised Inspector McManus and Agent Riportella that in December 2019, two customers, JF and SP, reported three checks which they did not write, were presented for payment and negotiated against their HELOC accounts. One check was in the amount of $59,000.00 and payable to "Harvest Company." The two other checks were in the amount of $34,500.00 made payable to VF and $29,000.00 made payable to SW. A review of the checks revealed they lacked a seal and specific wording that appear on genuine Pawtucket CU HELOC checks and were deemed counterfeit. The customers were contacted and stated they had not lost nor had any HELOC checks stolen and that they had received all their monthly statements. The checks were returned to the financial institutions that had negotiated them and the funds were returned to Pawtucket CU thus enabling Pawtucket CU to reimburse the customers.
13. On January 14, 2020, the Pawtucket CU Bank investigator was able to speak with two other financial institutions as well as an individual who received one of the aforementioned checks. The individual, later identified as JW, brought the check to his bank and had concerns regarding the legitimacy of the check due to his old account number being written on the front of the check. After confirming that the check was indeed legitimate, Regions Bank opened a new account for JW and placed a seven day hold on the check due to the customer's concern. The investigator stated to me from his conversations with JW, it appeared that he was an unwitting participant and that JW was advised by the investigator that law enforcement would be contacting him in the near future to gather additional information.
14. On January 15, 2020, I spoke to JW who had received the counterfeit Pawtucket CU HELOC check in the amount of $59,000 made payable to "Harvest Company". JW stated the check arrived via a USPS Priority Mail envelope which bore a return address in Providence, RI and which contained no other paperwork. JW believed the check was a donation to his church and attempted to deposit it at his bank. Several days later, JW was

notified that the check was indeed counterfeit. JW stated that, to this day, he has not received any correspondence from anyone regarding this check. On February 10, 2020 and March 5, 2020, follow-up calls and texts made to JW to collect additional information were met with negative results.

15. Using proprietary US Postal databases, I learned that the tracking number associated with the envelope mailed to JW was mailed from the Elmwood (RI) Post Office (PO) on December 23, 2019 between 11:14AM-11:17AM. Additionally, a receipt of the transaction revealed five additional envelopes were mailed to various individuals throughout the country on the same date and time. All six envelopes which were mailed out had the same weight (.0625 lbs.) and postage amount ($7.35). Video surveillance from the Elmwood PO on December 23, 2019, between 11:14AM-11:17AM, showed a black male with long braided hair wearing a gray sweater, later identified as PATRICK JOHNSON, conducting the transaction while talking on a cell phone. The receipt from the aforementioned transaction revealed that the transaction was paid for with a debit card issued to Whayee Sarkpah-Johnson of 211 Hanover Street, Providence, RI. The six mailings were addressed to the following individuals/company and Pawtucket CU bank records revealed counterfeit HELOC checks were also made payable to the same individuals/company around the same date of the mailings:

December 23, 2019 Mailings from Elmwood PO with JOHNSON on Surveillance Video

MAILING DATE	MAILING TIME	POST OFFICE	TRACKING #	SENDER NAME FROM MAILING ENVELOPE	ADDRESSEE NAME FROM MAILING ENVELOPE:	CHECK AMOUNT
23-Dec-2019	11:14-11:17 AM	ELMWOOD PO	9505511924419357268059	GEOFFREY LECAM	GD[2]	$68,500.00
23-Dec-2019	11:14-11:17 AM	ELMWOOD PO	9505511924419357268028	JOHN FRACASSO	HARVEST COMPANY	$59,000.00
23-Dec-2019	11:14-11:17 AM	ELMWOOD PO	9505511924419357268073	MARK ALBERT	KC	$52,000.00
23-Dec-2019	11:14-11:17 AM	ELMWOOD PO	9505511924419357268042	STEVEN GRAFF	MT	$72,000.00
23-Dec-2019	11:14-11:17 AM	ELMWOOD PO	9505511924419357268066	SUSAN BUTTRICK	ER[3]	$85,000.00

[2] On 11/19/19, an envelope (Tracking # 9505515251839323180854) containing a Union Bank & Trust HELOC check was mailed to GD from the Irvington (NJ) Post Office. On 11/21/19, GD deposited Union Bank & Trust #259 in the amount of $43,800.00 into his JP Morgan Chase Bank account.

[3] On 1/7/20, an envelope (Tracking # 9505512961420007296993) containing a Union Bank & Trust HELOC check was mailed to ER from the Waban (MA) Post Office. On 1/13/20, ER

23-Dec-2019	11:14-11:17 AM	ELMWOOD PO	9505511924419357268035	ILLEGIBLE	RD[4]	UNKNOWN

16. On January 30, 2020, Inspector Littlejohn (USPIS) and I responded to 211 Hanover Street in Providence, RI to interview Whayee Sarkpah-Johnson. Rhode Island DMV records also show Whayee Sarkpah-Johnson's address listed as 211 Hanover St, Providence, RI. I knocked on the front exterior door and a young female, who identified herself as Sarkpah-Johnson's daughter, informed me that her mother was at work. When questioned what this was regarding, I informed her that someone may be fraudulently using her mother's debit card. The young female asked if she could see a picture of the person using her mother's debit card to which we agreed. After reviewing a still image taken during the December 23, 2019 transaction at the Elmwood PO, the young female identified the individual as her father, Patrick JOHNSON.
17. Rhode Island DMV records for Patrick JOHNSON obtained subsequent to the interview confirmed JOHNSON is the same person from the December 23, 2019 transaction, and listed an address of 40 Sterling Ave, Providence, RI. A criminal check for JOHNSON revealed a 2010 federal conviction for felon in possession of a firearm for which he was sentenced to 37 months imprisonment with 3 years of supervised release and 2006 conviction for possession with intent to distribute a controlled substance for which he received a 5 year suspended sentence with 5 years of probation. In addition, I later identified the young female answering the door at 211 Hanover St. as Patricia JOHNSON by her RI DMV photograph. A criminal check for Patricia JOHNSON revealed no criminal history.
18. Further investigation revealed that three other financial institutions, Bethpage Federal Credit Union, Union Bank & Trust and Village Bank, reported customers who had their HELOC account information compromised. Additionally, several of these HELOC checks were sent to individuals who had either received a counterfeit Pawtucket Credit

---

deposited Union Bank & Trust #125 in the amount of $125,000.00 into his Bank of America account.

[4] On 11/20/19, an envelope (Tracking #9505510694119324226895) containing a Union Bank & Trust HELOC check was mailed by JOHNSON, as shown by PO surveillance video, to RD from the Olneyville (RI) Post Office. On 11/25/19, RD Union Bank & Trust #581 in the amount of $19,200.00 into his Carrollton Bank account.

Union check or a mailing from Patrick JOHNSON sent on December 23, 2019. One of the counterfeit Bethpage Federal Credit Union HELOC check included a check dated October 14, 2019, from M.A.'s account in the amount of $8,500.00 made payable to Individual #1. Individual #1 was later interviewed as more fully elaborated below and identified Patrick JOHNSON as the individual who had given her the counterfeit check.

19. A USPS address history review of individuals who received checks from one or more of the compromised financial institutions revealed almost all of them had received a mailing(s), similar in weight (.0625 lbs.) and postage amount ($7.35) around the same time the HELOC check was dated or deposited. Most of these mailing(s) were sent from post offices located in New Jersey, New Hampshire, Massachusetts, and Rhode Island.

20. One individual, identified as RD, who received a mailing from Patrick JOHNSON as part of the December 23, 2019 transaction referenced in paragraph 14, had previously received a mailing sent to him on November 20, 2019, from the Olneyville (RI) PO. The November 20, 2019, mailing, with a tracking number ending in 6895, contained Union Bank & Trust check #581 in the amount of $19,200.00 which was deposited into RD's Carrollton Bank account on November 25, 2019. The receipt from the postal transaction revealed three total mailings, each mailing costing $7.35 in postage and paid for in cash were mailed out between 2:34PM-2:36PM. Video surveillance from the Olneyville PO on November 20, 2019, between 2:34PM-2:36PM, revealed JOHNSON conducting the transaction. Video surveillance also showed JOHNSON with a cell phone appearing to make or receive several calls during this transaction and checking his phone while at the counter:

November 20, 2019 Mailings from Olyneyville PO with JOHNSON on Surveillance Video

MAILING DATE	MAILING TIME	POST OFFICE	TRACKING #	SENDER NAME FROM MAILING ENVELOPE	ADDRESSEE NAME FROM MAILING ENVELOPE:	CHECK AMOUNT
20-Nov-2019	2:34-2:36 PM	OLNEYVILLE PO	9505510694119324226895	Unknown at this time	RD	$19,200.00
20-Nov-2019	2:34-2:36 PM	OLNEYVILLE PO	9505510694119324226888	Unknown at this time	Unknown at this time	Unknown at this time
20-Nov-2019	2:34-2:36 PM	OLNEYVILLE PO	9505510694119324226871	Unknown at this time	Unknown at this time	Unknown at this time

21. Another individual, identified as SW, who received a counterfeit Pawtucket CU check from SB's account dated November 21, 2019 in the amount of $29,000.00 and made payable to SW, had received a mailing sent to her on November 26, 2019 from the Olneyville (RI) PO. The receipt from the postal transaction revealed two total mailings, each mailing costing $7.35 in postage and paid for in cash were mailed out between 2:33PM-2:34PM. Video surveillance from the Olneyville PO on November 26, 2019, between 2:33PM-2:34PM, showed JOHNSON conducting the transaction wearing a black shirt with the word "STACKS" in large white block lettering. Video surveillance also showed JOHNSON on his cell phone when he enters the post office and showed JOHNSON texting on his cell phone during the transaction:

November 26, 2019 Mailings from Olneyville PO with JOHNSON on Surveillance Video

MAILING DATE	MAILING TIME	POST OFFICE	TRACKING #	SENDER NAME FROM MAILING ENVELOPE	ADDRESSEE NAME FROM MAILING ENVELOPE:	CHECK AMOUNT
26-Nov-2019	2:33-2:34 PM	OLNEYVILLE PO	9505510694119330227572	Unknown at this time	SW	$29,000.00
20-Nov-2019	2:33-2:34 PM	OLNEYVILLE PO	9505510694119330227589	Unknown at this time	Unknown at this time	Unknown at this time

22. Another individual, identified as CA, who received two counterfeit Pawtucket CU checks, both dated December 12, 2019, had received a mailing sent to him on December 11, 2019, from the Irvington (NJ) PO. The December 11, 2019, mailing to CA, with a tracking number ending in 7130, had a return name of "Renee Johnson" with an address of 211 Hanover Street, 2nd Flr, Providence, RI 20907 and contained the following checks:

    a. Pawtucket FCU check #53 in the amount of $29,000.00 which was deposited into CA's National Bank of Texas account on 12/18/19.

    b. Pawtucket FCU check #81 in the amount of $31,200.00 which was deposited into CA's Wells Fargo account on 12/17/19.

    The receipt from the postal transaction revealed four total mailings, each mailing costing $7.35 in postage and paid for in cash.

23. Another individual, identified as GD, who received a mailing from JOHNSON as part of the December 23, 2019 transaction referenced in paragraph 14, had previously received a mailing sent to him on November 19, 2019, from the Irvington (NJ) PO. The mailing,

with a tracking number ending in 0854, contained Union Bank & Trust check #259 in the amount of $43,800.00 which was deposited into GD's Chase Bank account on 11/21/19. The receipt from the postal transaction revealed five total mailings, each mailing costing $7.35 in postage and paid for in cash were mailed out between 10:12AM-10:16AM.

24. On January 29, 2021, I interviewed an individual, identified as KC, who received a mailing from JOHNSON as part of the December 23, 2019 transaction referenced in paragraph 14. KC stated she met an individual on the dating site Zoosk a few weeks prior to receiving the check but couldn't recall his name. KC stated she wasn't expecting the check but when it arrived, she asked the individual what she should do with it. KC was instructed by the individual to deposit the check into her bank account and then transfer the funds to another bank account in New York. KC stated the transfer of funds never took place because the check was deemed counterfeit prior to her transferring any funds.

INTERVIEW OF INDIVIDUAL #1 WHOSE BANK ACCOUNT WAS USED TO DEPOSIT A COUNTERFEIT CHECK

25. On June 11, 2020, Individual #1 was interviewed by Postal Inspectors regarding a counterfeit check that was deposited into her bank account in RI. TD Bank records for Individual #1 showed that a counterfeit Bethpage Federal Credit Union (Bethpage FCU) check had been deposited into her account on October 21, 2019.
26. Individual #1 was shown the Bethpage FCU check dated October 14, 2019, in the amount of $8,500.00 made payable to her. Initially, Individual #1 indicated she did not recognize the check and stated she did not have an account at TD Bank. Individual #1 indicated that she had an account at TD Bank in the past, but someone had stolen her credit card. Individual #1 then admitted the check was deposited into her account at TD Bank and stated she received the check from Patrick JOHNSON. She described JOHNSON as a black male, dreadlocks and drove either a Toyota[5] or Honda.

[5] Surveillance video from the Elmwood Post Office on 12/23/2019 shows JOHNSON operating a later model Toyota Avalon. Additionally, surveillance of 211 Hanover St, Providence, RI has observed a 2006 Toyota Avalon (RI Tag #AS194) parked in the driveway. This vehicle is registered to JOHNSON's wife, Whayee Sarkpah-Johnson at 100 Eliza St., Providence, RI.

27. Individual #1 stated JOHNSON drove her, her ex-boyfriend, and another unidentified male to deposit the check at TD Bank in October 2019. Individual #1 described the unidentified male who accompanied JOHNSON as African, had dreads, and looked like JOHNSON. Individual #1 stated she watched JOHNSON fill out the front portion of the check, had her sign it and then JOHNSON deposited the check at the TD Bank drive-thru using Individual #1's debit card. When Individual #1 asked if she was going to get in trouble for this, she was informed that it was legit and to not ask too many questions.
28. Individual #1 stated after JOHNSON deposited the check at TD Bank[6], JOHNSON drove Individual #1 to the post office in Providence[7] to purchase money orders. Individual #1 stated she purchased two blank money orders, one for $900.00 and the other for $1,000.00, both of which she gave to JOHNSON.
29. Individual #1 stated while checking her bank account several days later, she noticed that the Beth Page FCU check she had received had cleared and the funds were still available in her account. Individual #1 admitted she withdrew the remaining amount, around $5,000.00, and used the money to pay her rent, make some purchases at Walmart and buy a vehicle.
30. Individual #1 also later showed me the unidentified male's Facebook page that had accompanied her, her ex-boyfriend, and JOHNSON in the car. The unidentified male had the Facebook username "Teebone Juheard" and corresponding Facebook profile photographs.
31. Individual #1, after providing a phone number for her ex-boyfriend, agreed to make a controlled phone call to her ex-boyfriend to validate her story. Individual #1 asked her ex-boyfriend if he remembered doing the check with Patrick (JOHNSON) to which her ex-boyfriend replied "yes". Individual #1 informed her ex-boyfriend that the bank wanted her to pay the money back, to which her ex-boyfriend instructed her to set up a payment plan. Individual #1 asked her ex-boyfriend for JOHNSON's phone number so

[6] Individual #1 stated during the interview that JOHNSON deposited the check at the TD Bank branch located on Mineral Spring Ave (North Providence, RI). Bank records revealed that the check was actually deposited at the TD Bank branch located at 180 Westminster St in Providence, RI.

[7] United States Post Office, 24 Corliss St, Providence, RI 02904

she could "do another check" to pay back the bank to which her ex-boyfriend replied "I don't talk to Patrick anymore".

32. A review of Individual #1's TD bank records obtained through a grand jury subpoena revealed the following activity:
    - On October 21, 2019, a deposit of the aforementioned check was made at TD Bank, located at 180 Westminster St, Providence, RI, at 11:24 AM.
    - On October 23, 2019, a debit card transaction for $1,903.40[8] was made at the US Post Office, located at 24 Corliss Street, Providence, RI.
    - On October 25, 2019, five (5) ATM withdrawals totaling $5,000.00 were made at TD Bank, located at 1923 Mineral Spring Ave, North Providence, RI.
33. USPS transaction records revealed USPS money orders 26209529853 ($1,000) and 26209529864 ($900) were purchased on October 23, 2019 at 10:13 AM by Individual #1 at the Main Post Office, located at 24 Corliss Street, Providence, RI with TD Bank debit card xxxxxxxxxxxx3988[9].
34. USPS transaction records revealed USPS money orders 26209529853 and 26209529864 were cashed on October 24, 2019 at 9:37 AM at the Elmwood Post Office, located at 820 Elmwood Avenue in Providence, RI. Money order images revealed the payor as Patrick JOHNSON of 40 Sterling Ave in Providence, RI and the payee as Patricia F JOHNSON of 211 Hanover, Prov, RI. A Rhode Island driver's license 21370677[10], which is Patricia JOHNSON's license number, was provided to complete the transaction and recorded by the USPS clerk on both of the money orders.
35. Using law enforcement databases and open social media pages, we were able to identify "Teebone Juheard" as Terrance RICHARDSON. A photo of RICHARDSON was sent to Individual #1 who confirmed RICHARDSON was Teebone Juheard. A criminal history check for RICHARDSON revealed a 2018 state conviction for forgery and counterfeiting for which he received a 5 year sentence, 18 months to serve with 42 months suspended,

[8] There is a $1.70 service fee for money orders over $500 and up to $1,000.

[9] TD Bank account records revealed debit card xxxxxxxxxxxx3988 is associated with Individual #1

[10] Rhode Island DL 21370677 is assigned to Patricia F. JOHNSON of 211 Hanover St, Providence, RI.

and 42 months' probation. RICHARDSON also has a pending unlawful breaking and entering of a dwelling house charge in the RI state court.

INTERVIEW OF INDIVIDUAL #2 WHOSE BANK ACCOUNT WAS USED TO DEPOSIT A COUNTERFEIT CHECK

36. On October 23, 2020, Individual #2 was interviewed by Postal Inspectors regarding a counterfeit check deposited into her bank account in RI.
37. Individual #2 was shown a Union Bank & Trust check dated November 3, 2019, in the amount of $8,700.00 made payable to her. Initially, Individual #2 indicated she did not recognize the check and later changed her story stating she lost her debit card. Individual #2 then admitted she met a guy on Facebook under the name "Sunnyboy Taylor" who she gave her debit card and PIN to. Individual #2 stated that his real name is Richard KOBOI and showed me his Facebook page on her phone. Individual #2 stated KOBOI was posting advertisements on Facebook looking for bank accounts to deposit checks into in exchange for cash. Individual #2 acknowledged that KOBOI met her in North Kingstown, RI and was driving an older model Toyota Camry. Individual #2 stated KOBOI took her card and handled the transaction by himself. Individual #2 stated she only found out about the deposited checks after Bank of America notified her about her account being closed due to the counterfeit check. Individual #2 stated she never received any money from KOBOI because the check never cleared.
38. Individual #2 was questioned regarding other co-conspirators in this investigation, including Terrance RICHARDSON. Individual #2 stated she knew Terrance RICHARDSON. When questioned further about her relationship with RICHARDSON, Individual #2 stated she knew him from her neighborhood but added she never did business like that. When asked if she was friends with RICHARDSON on Facebook, she stated no. When questioned further regarding being friends with anyone named "Teebone" on Facebook, she said yes but stated she doesn't understand why that mattered. In addition, Individual #2 refused to allow us to see RICHARDSON's Facebook account under the name "Teebone Juheard".
39. On October 15, 2020, the Honorable Lincoln D. Almond signed a search warrant (20-SW-378-LDA), authorizing the search of Facebook records for Facebook Name "Teebone Juheard" (20-SW-378-LDA).

40. Facebook records for "Teebone Juheard", received after our conversation with Individual #2, revealed a conversation between Individual #2 and "Teebone Juheard" that took place on June 3, 2019. Below is their Facebook conversation in its entirety:

> *Individual #2: Td bank ?*
> *Teebone Juheard: Yea but it's gunna be for like 3500*
> *Individual #2: Does it matter how long the bank been opened ?*
> *Teebone Juheard: Should be 30 days longer*
> *Individual #2: Ok*

41. Based upon my training and experience, this conversation is directly related to check fraud. I am aware that individuals using the banking system to commit fraud often prefer established bank accounts over newly created accounts because the banks often utilize more rigorous fraud mechanisms against newly created accounts. This enables an established account holder to have the ability to defraud a bank of more money than a newly created account would be able to do.

INTERVIEW OF INDIVIDUAL #3 WHOSE BANK ACCOUNT WAS USED TO DEPOSIT A COUNTERFEIT CHECK

42. On January 8, 2021, Individual #3 was interviewed by Postal Inspectors regarding a counterfeit check that was deposited into her bank account in RI.

43. Individual #3 acknowledged allowing someone to use her Navy Federal Credit Union (CU) account to deposit a check into. Individual #3 stated during that time, her unemployment ran out and she needed the money. Individual #3 stated she responded to a Facebook advertisement from a guy "Sunnyboy" who promised to give her a 50/50 cut if she let him use her account. Individual #3 hesitantly agreed and met "Sunnyboy" in a park to give him her debit card and PIN. Individual #3 stated he was driving a larger model black SUV and was by himself. Individual #3 stated she didn't know his real name and she tried to find him later on Facebook, but his account was deactivated. Individual #3 stated "Sunnyboy" took her card and handled the transaction by himself. Individual #3 stated she only found out about the counterfeit check after speaking to someone at Navy Federal CU about her account. Individual #3 stated she lost over $18,000.00 due to the counterfeit check, didn't receive any money from the check, and is in the process of paying back Navy Federal CU.

44. Individual #3 was questioned about other people involved in this scam and stated that she ApplePay'ed money to people other than "Sunnyboy". Individual #3 stated that "Sunnyboy" was always on the phone talking to some African guy with an accent. Individual #3 reluctantly agreed to assist with the investigation any way she can to keep herself out of trouble but was worried about her own safety.
45. On January 8, 2021, I spoke with a Navy Federal CU bank investigator who confirmed a fraudulent check for $22,308.50 was mobile deposited on October 20, 2020 into Individual #3's Navy Federal CU bank account. The Navy Federal CU bank investigator stated the payor of the check was the Law Office of Robert V. Russo and the payee was Individual #3. The investigator also confirmed that IP 172.56.23.59 was associated with the mobile deposited check and was the historical IP assigned to the account - meaning Individual #3 most likely deposited the check herself. The investigator confirmed there multiple fund transfers from Individual #3's account to various individuals, via Cash App and PayPal, totaling $18,250.05.
46. On December 2, 2020, the Honorable Lincoln D. Almond signed a search warrant (20-SW-438-LDA), authorizing the search of Facebook records for Facebook Name "Sunnyboy Taylor" (User ID richard.koboi) for basic subscriber information, IP address logs, messages, photos, transactional information, videos, and other content and records. Facebook records for KOBOI using the Facebook Name "Sunnyboy Taylor" revealed a conversation that KOBOI had with Individual #3 discussing depositing a counterfeit check into Individual #3's bank account on October 14, 2020. On October, 20, 2020, KOBOI sent a Facebook message to Individual #3, "come to 539 Dexter St". When Individual #3 stated that she is "here," KOBOI responded that "give me one second, having my moms house remodeled inside." KOBOI'S Facebook records also showed that Individual #3 sent screenshots of a mobile deposit submitted in the amount of $22,308.50 which was deposited into the Navy Federal CU account and then a subsequent screenshot showing the deposit had been declined because it was missing a special endorsement on the back of the check. Subsequently, KOBOI sent a Facebook message for Individual #3 to call his phone.

FRAUDULENT CREDIT CARD APPLICATION ASSOCIATED WITH PATRICK JOHNSON

47. In March of 2020, US Bank investigators made me aware of an identity theft issue involving Patrick JOHNSON. The issue related to a credit card application in the name of victim DB and using DB's social security number and date of birth that was submitted on October 28, 2019. The application was submitted via the internet from IP address 194.36.111.106. The application which identified JOHNSON as an authorized user, lists a mailing address of 211 Hanover St, Providence, RI. Additionally, the email address Fainb659@gmail.com and cell phone (518) 952-5575 were listed as the primary contact information on the application. Bank investigators confirmed that both the victim's government issued SSN and actual DOB along with Patrick JOHNSON's name as an authorized user and JOHNSON's purported but false SSN and DOB[11] were submitted as part of the application process. The victim DB confirmed it was fraudulent on November 15, 2019 and the application was denied on November 19, 2019. No credit card was ever opened, and US Bank did not incur a loss as a result of the activity.
48. On June 4, 2020, I spoke to DB and her husband MB who stated they knew nothing about a credit card being opened under her name. DB stated she didn't know anyone named Patrick JOHNSON and that the phone number (518-952-5575) and email address (fainb659@gmail.com) listed on the application did not belong to her. DB recalled having an issue last year regarding someone cashing checks written on their home equity loan but didn't recall it being related to a credit card. MB stated there were two checks written on his HELOC loan with Union Bank[12]. MB stated that after the incident, he froze both his and his wife's credit and now monitors their credit reports regularly. MB confirmed that his wife never applied for a credit card with US Bank.
49. Subscriber records for telephone number (518) 952-5575, believed to be Patrick JOHNSON's phone, revealed it is associated with T-Mobile Account and began service

[11] The SSN ending in 8110 and DOB (8/20/79) listed on the credit card application are not associated with JOHNSON.

[12] Union Bank & Trust records revealed two checks (#203 & #416) in the amounts of $65,000 and $9,600, written against MB & DB's HELOC account on November 1, 2019 and November 3, 2019.

on April 1, 2019 and was deactivated on February 29, 2020. There is no subscriber name, subscriber address, billing name or billing address associated with this account.

50. Between April 1, 2019 and February 29, 2020, T-Mobile toll records for (518) 952-5575, believed to be Patrick JOHNSON's phone, revealed 148 incoming calls and 159 outgoing calls to (401) 499-7593,[13] believed to be used by Patrick JOHNSON's wife. Additionally, there was an outgoing call on November 21, 2019, from the number for Individual #1's ex-boyfriend who was involved in the counterfeit check deposit described in paragraph 32.[14]

51. Gmail records revealed email account fainb659@gmail.com was created on February 2, 2019 under the name Barry Fain. An account recovery email address of cowger659@yahoo.com and a recovery phone number of (347) 230-7119 were provided during the account creation. Additionally, on October 29, 2019, a day after the fraudulent credit card application was submitted, there was login and logout activity related to the fainb659@gmail.com email account from IP 194.36.111.106. This is the same IP that was captured on October 28, 2019 by US Bank related to the credit card application referenced in paragraph 47.

52. Subscriber records for telephone number (347) 230-7119 revealed it is associated with MagicJack[15] Account 50765904 and began service on September 19, 2018 under the name Robert Royal. Under the list locations where the MagicJack is being utilized, it

[13] Sprint records for phone number (401) 499-7593 revealed it is assigned to Patrick JOHNSON, 211 Hanover St, Providence, RI 02909 and was established on 7/7/18. In addition, KOBOI's Facebook records show that (401) 499-7593 is the phone number provided by "Felicia Sarkpa Johnson" to KOBOI in a Facebook message. Facebook profile photos for "Felicia Sarkpa Johnson" compared to Whayee Sarkpa Johnson's DMV photo appear to be the same individual.

[14] As referenced above, Individual #1 made a controlled phone call to her ex-boyfriend at (401) 215-0839.

[15] MagicJack is a USB phone adapter that allows you to bypass traditional phone services and make calls via Voice over Internet Protocol (VoIP) to regular cell phones, landline phones or other VoIP users from a home, hotel room and even other countries. This technique used by scammers, commonly referred to as "phone spoofing", allows the caller to deliberately falsify the information transmitted to the victim's caller ID to disguise their true identity and location.

lists Glenn Wilson, 211 Hanover St, Fl 2, Providence, RI[16]. Additionally, one of the credit cards associated with the Magic Jack Account 50765904 belongs to Glenn Wilson at the aforementioned address.

RICHARDSON "TEEBONE JUHEARD" FACEBOOK RECORDS USED TO COMMUN ICATE WITH CO-CONSPIRATORS AND TARGET PHONE #1

53. Facebook records for "Teebone Juheard" revealed that the account was created on February 9, 2015. Facebook confirmed it is still an active Facebook account and phone number (401) 677-9165, TARGET PHONE #1, was verified by Facebook on May 28, 2020[17].

54. As further elaborated below, Facebook records for "Teebone Juheard" responsive to that search warrant show that "Teebone Juheard" communicated with the various co-conspirators to cash/deposit counterfeit checks, obtain information for cashing/depositing counterfeit checks, and/or produce paper stock for counterfeit checks.

55. Facebook records for "Teebone Juheard" revealed that this account was used to advertise and solicit co-conspirators to engage in the bank fraud scheme. For example, a photo posted on April 4, 2020 of a Bank of America receipt that states "5k next day – 10k two business days – All Bank of America HMU – Teebonejuheard". Additionally, in a Facebook Messenger conversation on October 6, 2019, Individual #4 sent a screen shot of "Teebone Juheard" Facebook's account to him in which he posted "YKTVS[18] whoever tryna make 9k next day DM ME" along with photographs of cash and a Bank of America receipt. The two then have the following conversation:

> *Individual #4: So wusss da word ?*
> *Teebone Juheard: What's good*
> *Individual #4: I gotta BOA card but I'm not trynha get into dat fraudulent ish & get played .*
> *Teebone Juheard: Listen for one I know what I'm doing and two this is how I feed my family my kids why would I play you*

[16] A search of USPS and law enforcement databases for Glenn Wilson at 211 Hanover St, Providence, RI was met with negative results.

[17] "Verified" indicates the account holder responded to a text sent to the listed phone number.

[18] YKTVS is slang for You Know The Vibes

Individual #4: I'm jus being on my safe side as well as yu would be , I seen ya pics & what come back in so I'm jus trynha see what's good & when we can get shit popin ,
Teebone Juheard: My bad game day been busy but tomorrow
Teebone Juheard: Hey if you wanna do it I can meet with you and give you the slip so you can deposit it on your own so you can feel safe like I'm not gunna play you just have to keep me updated
Individual #4: Aight bett I'll let you know when I'm free to meet up .
Individual #4: Cause I have work
Teebone Juheard: Iight send your name and address that's on the account I'll have it printed up

56. Facebook records for "Teebone Juheard" also revealed a conversation with Individual #5 that took place on September 28, 2020.

Teebone Juheard: Who you fucking up ?
Individual #5: Fuck I gotta lie about ! Bring my shit back . My account is all fucked Up for nothing. You don't bring my shit ima see you point blank. I ain't no kid I'm a grown ass man playa . I kept my word on everything that was asked of me
Teebone Juheard: But who you fucking up is what I'm asking
Individual #5: You want to meet up ?
Teebone Juheard: Yea come get it.

"Teebone Juheard" then sent a photograph of a Santander debit card in Individual #5's name next to what appears to be a firearm and a magazine containing ammunition based upon my training and experience. On December 1, 2020, I interviewed Individual #5. Individual #5 stated he has never met RICHARDSON and provided his debit card and PIN to a mutual friend. Individual #5 was told by his friend that RICHARDSON needed to use his bank account to deposit a legitimate check into it. Individual #5 stated that he never actually saw the check that was deposited into his account. After Individual #5 was notified by Santander that the check was fraudulent, he asked for his debit card back. Individual #5 stated RICHARDSON sent him a photo over Facebook of his debit card along with a handgun and told him "Yea come get it". Individual #5 stated he has yet to recover his debit card from RICHARDSON and has not communicated with RICHARDSON since**.** Santander provided the check deposited into Individual #5's account which shows a check made payable to Individual #5 in the amount of $15,930.00, allegedly endorsed with Individual #5's signature on the back.

57. Facebook records for "Teebone Juheard" also revealed a conversation that took place on October 1, 2019 with Individual #6 regarding making and printing counterfeit checks. Below is a summary of their conversation:

Individual #6: I need in . . .
Teebone Juheard: What account you have
Individual #6: Bank of America or I will open one if u need me to
Teebone Juheard: Yea that Bank of America is good
Teebone Juheard: You tryna do it today?
Individual #6: I bounced some checks last week
Individual #6: But I am down
Teebone Juheard: They cleared?
Teebone Juheard: You bounces them in your account?
Individual #6: Wrote them out in the store
Teebone Juheard: Does that have anything to do with your account?
Individual #6: We can try if you wanna
Teebone Juheard: Iight send your name and address that's on the account imma print them up
*Individual #6: **sends name and address***

58. Facebook records for "Teebone Juheard" also revealed a conversation that took place on June 3, 2019 with Individual #7 regarding printing and depositing counterfeit checks. Below is a summary of their conversation:

Individual #7: I need in
Teebone Juheard: What bank you have
Individual #7: Citizens
Teebone Juheard: How long it's been open
*Individual #7: Only **
Teebone Juheard: What's a couple months?
Individual #7: Four/five months
Teebone Juheard: Do you use it
Individual #7: My checks get deposit into it but I haven't worked since the second week of May
Individual #7: But um idk guess let me know if not it's all gd .. you be safe but I seen numbers nd I don't mind doing what needed to get it ..
Teebone Juheard: Iight so basically you have to walk in and deposit the check thru the teller
Teebone Juheard: And it'll clear tomorrow morning
Individual #7: Ok then what
Teebone Juheard: Then we link when it clear go to the casino and cashout
Individual #7: Okay well Let me Know when and I'm in
Teebone Juheard: Send your name and address that's you use to open the account
Teebone Juheard: Imma print it and meet up with you
*Individual #7: **sends address***

Individual #7: Well I hope it works nd then idk let's talk about my cut nd obviously you get you're big I need a come up real quick just to buy a whip cause my husband took all my shit and left me with nothing
Teebone Juheard: Imma do 7500 you get 3 cuz imma pay the person who get the checks out my cut
Teebone Juheard: Your fb name is your real name
Individual #7: Yes it is
Individual #7: I know you obviously do this but what's this check from or etc
Individual #7: Cause I have 25 yrs over my head can't afford shit to slip up but I kno you'll probably tell me how to go about it
Teebone Juheard: Iight nothing gonna happen
Teebone Juheard: It's from a job where they work with mental illness kids
Individual #7: So how I take it all out at once
Teebone Juheard: Iight call me

59. Facebook records for "Teebone Juheard" revealed a conversation between Individual #8 and "Teebone Juheard" that took place on September 23, 2020, in which RICHARDSON provides Individual #8 with the number for TARGET PHONE #1. Below is a summary of their Facebook conversation which based on my training and experience is a discussion relating to bank account information for the purpose of depositing counterfeit checks:

Individual #8: Send me your number
Teebone Juheard: Why what's up
Individual #8: Obviously something
Teebone Juheard: Didn't you have it
Individual #8: My home girl has boa[19]
Teebone Juheard: 4016779165
Individual #8: Yo
Individual #8: You do chase ?
Teebone Juheard: Yea
Individual #8: Ok
Individual #8: If it's 2 different accounts they won't close both of them right
Teebone Juheard: Are you tryna make money or what

[19] BOA is an abbreviation for Bank of America

KOBOI "SUNNYBOY TAYLOR" FACEBOOK RECORDS
Facebook Communications with Co-Conspirators

60. Facebook records for "Sunnyboy Taylor" revealed that the account was created on June 28, 2010. Facebook confirmed the account was deactivated on November 27, 2020.

61. As further elaborated below, Facebook records for "Sunnyboy Taylor" responsive to that search warrant show that "Sunnyboy Taylor" communicated with the various co-conspirators to cash/deposit counterfeit checks, and obtain information for cashing/depositing counterfeit checks.

62. Facebook records for "Sunnyboy Taylor" revealed that this account was used to advertise and solicit co-conspirators to engage in the bank fraud scheme. For example, three photos sent using this Facebook account on January 8, 2020 displayed stacks of US currency followed by "ALL CITIZENS BANK ACCOUNT HOLDERS HMU TODAY – CRANSTON, RHODE ISLAND – 50/50 SPILT(sp)".

63. Facebook records for "Sunnyboy Taylor" also revealed a conversation with Individual #9 that took place between October 30, 2020 and November 3, 2020 which is summarized below and describes how the counterfeit check fraud scheme worked:

> *Sunnyboy Taylor: What you need*
> *Individual #9: How Much we talkin bro last time I did this shit I got burned my account went negative and I ain't get shit but I feel like I can trust yohb*
> *Sunnyboy Taylor: I ain't moving like them niggas is moving bro , that's why they ain't last. I do business based off loyalty and trust alone . Who youbanking with*
> *Individual #9: Citizens*
> *Sunnyboy Taylor: How long have you been banking with them*
> *Individual #9: Couple months now*
> *Sunnyboy Taylor: Okay, so basically what I do is simple. I want you to know what it is I do isn't legal but it's safe. This isn't something where you have to worry about cops or your bank and credit . I do business with individuals who have good history with there banks. I make typed up or written checks from offshore 300k plus accounts . That type up or written check will be made out to you where we will then deposit it into your account . Usually it days one business day to two the most for the money to be available. Once the account shows that the money is there we will then take the steps needed to take the money out of the account. We will then spilt 50/50. No middle man or bad blood. You will still be able too use and keep your account as well as do it again in the future if you please. Let's eat*

Individual #9: I'm with it but it'll have wait till after this week I got some bills that come out as autopay and I don't want nothing to happen so I'll hit you up Friday cause I get paid Thursday if that works for you. And how much bread we talking?
Sunnyboy Taylor: Whenever your ready we will talk business and talk numbers
Individual #9: Aye bro I'm ready get some bread but please bro I got burned and a lot of bad shit happened last time I did this I can't bank with centrism banks because of the last time I trusted someone with this shit bro you're a brother I feel like you're honest if not that's cool get your bread but if it Fuccs up my account bro I don't wanna do it you feel me but if it's gonna be good I'm all for it
Sunnyboy Taylor: Honestly bro, I don't go around burning people, I keep my name clean and my business cleaner. I do business based off loyalty and trust. If you put your trust in me and do as I say bro. We can make it happen. I'm a man like you a man. Wouldn't disrespect you or cross the line g. I can't get the racks with out you. I ain't got timetoo be playing with money. That's my word you in good hands
Sunnyboy Taylor: Let's eat
Individual #9: let's get it what I need to do?
Sunnyboy Taylor: Text me
Sunnyboy Taylor: 4015439323

In a later Facebook conversation from August 1, 2020, Individual #9 asks KOBOI to make him plates and insurance for his car and provides his full name for this purpose as requested by KOBOI.

64. A review of bank records related to Individual #9's Citizens Bank account ending in 4285 revealed on November 4, 2020, a Union Bank & Trust check[20] in the amount of $9,600.00 was deposited into Individual #9's account at the Citizen's Bank Washington Park ATM in Providence, RI. The check was made payable to and endorsed by Individual #9. A review of the check revealed it was counterfeit and was returned as fraudulent on November 7, 2020. Prior to the check being returned as fraudulent, Individual #9 was able to obtain approximately $823.08 of the funds from the account via ATM withdrawals and debit card purchases.

KOBOI's Communications with Patricia JOHNSON to Deposit Counterfeit Check and Target Phone #3

[20] The payors of Union Bank & Trust check #416 was MB and DB of Williamsburg, VA. As detailed above, DB's HELOC account was not only compromised by KOBOI by the use of the counterfeit check drawn on DB's HELOC account, DB was also victim of identity theft related to Patrick JOHNSON around the same time.

65. Facebook records for "Sunnyboy Taylor" also revealed a conversation with "Tricia Johnson" that took place on January 23, 2020 which is summarized below:

Sunnyboy Taylor: you still tight on money ? I have a way me and you can eat with your account but you have to keep it between us. The way I'll do it is the same way I did my very own personal citizen account
Tricia Johnson: Lol once isn't bring trouble to me you we good
Sunnyboy Taylor: It won't cause, lol only trouble is your dam father 😂 know him. But do you have a joint account with them or it's just your account ?
Tricia Johnson: Is my account
Sunnyboy Taylor: You have the can correct ?
Sunnyboy Taylor: How long have you had it
Tricia Johnson: 2 to three
Sunnyboy Taylor: Years?
Tricia Johnson: Yes
Sunnyboy Taylor: Okay yes cuz, I can do today. We eat tomorrow morning or even before the morning breaks if you have cash app and Apple Pay connected to your account
Tricia Johnson: I have cashapp connected to it
Sunnyboy Taylor: You have a IPhone right ?
Tricia Johnson: You sure it will not bring trouble right ?
Tricia Johnson: Yeah
Sunnyboy Taylor: Cuz, if I even thought for a spilt second you would be in trouble with the law , I would dare
Tricia Johnson: Ok
Tricia Johnson: Let get it tho
Sunnyboy Taylor: Okay we can do it today
Sunnyboy Taylor: Where you at ?
Sunnyboy Taylor: There's info I will need to make the check and complete
Tricia Johnson: Home
Sunnyboy Taylor: Okay send me your Full name on the card Address Online banking user name and password Card and pin.I will come get your card go make the deposit so you are no way in site
Sunnyboy Taylor: But to do this you may have to stay up late
Tricia Johnson: Patricia Johnson 211 Hanover st Providence
Sunnyboy Taylor: I will let you know when I'm outside cuz
Tricia Johnson: I'm about to leave the house tho
Sunnyboy Taylor: Hide the card outside somewhere for me then cuz and trust I will handle everything and let you know every step
***
Tricia Johnson: Lol hope my dad don't know about this
Sunnyboy Taylor: Shit I hope he don't too, but we gone play it safe as possible trust me.
Tricia Johnson: When you getting the card make sure he don't see you lol
Tricia Johnson: But I will soon go home

***
Sunnyboy Taylor: Pulling up cuz
Tricia Johnson: Just get it from the mailbox fast
Sunnyboy Taylor: Got it cuz

Subsequently in this Facebook correspondence, Patricia JOHNSON sent KOBOI what appears to be a phone screenshot of her bank accounts showing the balance of $56.79 for a non-interest savings account xxx4513 and of $100.75 of a student checking account xxxx0873, as well as messages that included her pin to the bank card and last four digits of her social security number. After Patricia JOHNSON sent KOBOI this information, KOBOI sends a Facebook message stating, "Text my number cuz," and "4015439323." Toll records for Patricia JOHNSON's phone number, TARGET PHONE #3, show that Patricia JOHNSON called KOBOI right after this Facebook message was sent.

66. TARGET PHONE #3 is believed to be Patricia JOHNSON's phone number because in a Facebook message on June 30, 2020, KOBOI asked Patricia JOHNSON to send her number and Patricia JOHNSON responded, "4016485717," which is TARGET PHONE #3. T-Mobile records responsive to a grand jury subpoena for TARGET PHONE #3 for subscriber information show that there is no subscriber name, subscriber address, billing name or billing address associated with this account.

67. Facebook profile photos for "Tricia Johnson" compared to Patricia JOHNSON's DMV photo appear to be the same individual that I spoke to at 211 Hanover St. on January 30, 2020. Additionally, a photo posted June 16, 2019 from Facebook username "Tricia Johnson" appears to show Patricia JOHNSON next to her father Patrick JOHNSON.

68. Citizens Bank records for Patricia JOHNSON's Citizens Bank Account #XXXXXX0873, on January 23, 2020, check #732831 from Providence Mutual in the amount of $8,352.16 was deposited into Patricia JOHNSON's Citizen's Bank account. The check was made payable to and endorsed with Patricia JOHNSON's name. A review of the check revealed it was counterfeit and was returned as fraudulent on January 24, 2020. Prior to the check being returned as fraudulent, approximately $4,500 of the funds from the account was taken out of the account via ATM withdrawals and debit card purchases.

KOBOI's Use of TARGET PHONE #2

69. Facebook records for "Sunnyboy Taylor" revealed a conversation between Individual #10 and "Sunnyboy Taylor" that took place between November 19, 2020 and November 23,

2020, which showed KOBOI's current phone number is TARGET PHONE #2. During the conversation about printing a counterfeit check and then using Individual #10's TD Bank account to deposit the check, KOBOI provides Individual #10 with the number for TARGET PHONE #2.

70. Records received from T-Mobile pursuant to a Grand Jury subpoena revealed phone number (267) 854-9972, TARGET PHONE #2, is registered as a Tracfone, therefore there is no subscriber information associated with the phone number. Records revealed an activation date of November 18, 2020 and shows it's still an active account. Additionally, phone calls made as recently as January 27, 2021, to TARGET PHONE #2 revealed that the number is still in service.

KOBOI's Facebook Communications Regarding Possessing Guns and Selling Guns

71. KOBOI's Facebook records further show communications that he possessed guns and that he has advertised guns for sale. For example, on November 8, 2020, a Facebook message was sent to KOBOI stating, "Take this down bro Yk them ppl b watching," to which KOBOI responds, "all my guns registered too me." In addition, on November 9, 2020, in response to message KOBOI receives telling him, "if thang ain't legit then take this pic down lil bro. You never know who watching and I don't want anything to happen to you because of a possible mistake ya heard?," KOBOI responds, "wouldn't even play like that . all my gun definitely under my name."

72. On August 13, 2020, KOBOI states in Facebook messages, "How I try to get you and I paid for your weed dude," and "Let me tell you that if I would of wanted to rob you I'd put my gun in your face."

73. On June 13, 2020, KOBOI sends photographs of what appears to be guns to an individual based upon my training and experience. In one of the photographs with a gun with a serial number are the words, "Forsale." In this same Facebook conversation, KOBOI states, "But the guns I got plenty." When asked if "Those for sale. . . 357? 40?" KOBOI responds, "Yessir." Based upon my training and experience, 357 and 40 refer to gun caliber.

TERRANCE RICHARSON's CHASE BANK ACCOUNT ENDING IN #3190

74. Chase Bank records show that Terrance RICHARDSON opened Chase Bank accounts #XXXXX3190 on October 17, 2019 and #XXXXX9727 on July 1, 2020. The accounts

were held in his name with an address of 21 Milk St #1, Providence, RI 02905. According to account opening documents, Terrance RICHARDSON provided a tax identification number (SSN) of XXX-XX-7567 and RI driver's license #21313972[21] as verification. Chase Bank closed account #XXXXX3190 on August 14, 2020 and account #682629727 on August 25, 2020.

75. A review of activity on the account revealed between April 14, 2020 and July 9, 2020, six counterfeit checks totaling $115,877.69, made payable to Terrance RICHARDSON were deposited into Chase Bank accounts #XXXXX3190 and #XXXX9727 via ATM deposits at the Chase Bank branch located at 234 Thayer St, Providence, RI, which was the same Chase Bank branch where the account was initially opened by RICHARDSON.
76. Prior to the checks being returned as fraudulent, RICHARDSON was able to obtain approximately $42,547.66 of the funds from the accounts via debit card transactions, ATM and over the counter cash withdrawals, Chase QuickPay and Zelle[22] money transfers to various bank accounts.
77. Surveillance photographs and video provided by Chase Bank show RICHARDSON making several of the aforementioned cash withdrawals in Rhode Island and New York. Additionally, a gold chain with a "TEE BONE" diamond pendant worn by RICHARDSON in some of the surveillance photos is identical to the gold chain and diamond pendant he is wearing in several photos on his Facebook page.

RICHARD KOBOI's WELLS FARGO BANK ACCOUNTS ENDING IN #0176 & #2175

78. Wells Fargo records show that Richard KOBOI opened Wells Fargo Bank accounts #XXXXXX0176 on February 18, 2020 and #XXXXXX2175 on March 5, 2020. The accounts were held in his name with an address of 2 Bodell Ave, Apt 6, Providence, RI 02909. According to account opening documents, Richard KOBOI provided a tax identification number (SSN) of XXX-XX-1348 as verification. These accounts were closed by Wells Fargo Bank on June 12, 2020.

[21] According to RI DMV records, RI driver's license #21313972 is associated with Terrance RICHARDSON, 21 Milk St, Apt 1, Providence, RI 02905.

[22] Chase QuickPay and Zelle are person-to-person payment services that lets you send and receive money from anyone with a U.S. bank account using an email address or mobile number.

79. A review of activity on the account revealed that on April 8, 2020, two counterfeit checks in the amounts of $2,896.43 and $6,597.77 and made payable to Richard KOBOI were deposited into KOBOI's Wells Fargo accounts #XXXXXX0176 and #XXXXXX2175 respectively via ATMs at the following Wells Fargo branch in Wilmington, DE. On April 9, 2020, a counterfeit check in the amount of $5,000.00 was deposited into Wells Fargo account #XXXXXX2175 at the Wells Fargo branch in Old Saybrook, CT.
80. Surveillance photographs provided by Wells Fargo show KOBOI making the aforementioned deposits in Delaware and Connecticut, and one of the subsequent withdrawals in Connecticut. Additionally, a gold chain worn by KOBOI in one of the surveillance photos is identical to a gold chain he is wearing in several photos on his Facebook page.
81. Prior to the checks being returned as fraudulent, KOBOI was able to obtain approximately $9,131.19 of the funds from the account via ATM withdrawals, debit card purchases, and Zelle transfers.A criminal history check for KOBOI included a 2018 conviction for receiving stolen property by false pretenses and personation and conspiracy for which he received a sentence of 5 years with 18 months to serve and 3 years, 6 months suspended and 5 years' probation; a 2016 conviction for breaking & entering for which he was sentenced to 5 years suspended, 5 years' probation; a 2016 conviction for domestic assault for which he was sentenced to 1 year suspended, 1 year probation; and an active warrant issued in Delaware for larceny from banking.
82. On October 27, 2020, I spoke with Detective Doug Shatley from the Delaware State Police regarding his investigation and active warrant for KOBOI. Detective Shatley stated he spoke to KOBOI on the phone regarding the counterfeit checks to which KOBOI denied ever having a Wells Fargo bank account. When confronted with ATM video of him depositing the checks, KOBOI stated he needed to speak with his attorney and would plan on turning himself in to the Troop 2 Barracks. As of the date of this affidavit, KOBOI has not turned himself in.
83. Notably, KOBOI's Facebook records show the following message from KOBOI on November 30, 2020, which appears to reference the Delaware counterfeit check: "Last one you gave me was a flop man. And they ended up arrest my peoples out there in Delaware."

RICHARD KOBOI's BANK NEWPORT ACCOUNT ENDING IN #7349

84. Bank Newport records show that Richard KOBOI opened Bank Newport account #XXXXXXXX7349 on June 9, 2020. The account was held in his name with an address of 2 Bodell Ave, Apt 6, Providence, RI 02909.

85. A review of activity on the account revealed between July 6, 2020 and July 30, 2020, KOBOI received six ACH credits, totaling $5,685.00, from three different government entities as detailed below:

Customer Account	Code	Date	Total Value	Description	Method
XXXXXXXX7349	XDEP	13-Jul-20	$1,500.00	SBAD TREAS 310 MISC PAY RMT*CT*	ACH
XXXXXXXX7349	XDEP	15-Jul-20	$867.00	MA DUA MA PUA PROGRAM CARES ACT	ACH
XXXXXXXX7349	XDEP	22-Jul-20	$867.00	MA DUA MA PUA PROGRAM CARES ACT	ACH
XXXXXXXX7349	XDEP	29-Jul-20	$867.00	MA DUA MA PUA PROGRAM CARES ACT	ACH
XXXXXXXX7349	XDEP	30-Jul-20	$867.00	MA DUA MA PUA PROGRAM CARES ACT	ACH
XXXXXXXX7349	XDEP	6-Jul-20	$717.00	STATE OF ARIZONA BENEFITPAY	ACH
TOTAL			$5,685.00		

On or around July 27, 2020, KOBOI was contacted by Bank Newport management in regard to the questionable ACH deposits in his account. KOBOI stated that Ma Dua Ma Pua was his sister, SBAD was his business that he applied for a loan with and that he use to work in Arizona for a company called Matrix thru December of 2019. It should be noted that MA DUA MA PUA is an acronym for Massachusetts Department of Unemployment Assistance / Massachusetts Pandemic Unemployment Assistance and SBAD is an acronym for Small Business Administration. Based on his KOBOI's inability to provide a valid explanation, Bank Newport decided to close KOBOI's account.

KOBOI's CHASE BANK ACCOUNTS ENDING IN #3426 & #3608

86. Chase Bank records show that Richard KOBOI opened Chase Bank accounts #XXXX3426 and #XXXXXX3608 on February 9, 2020. The accounts were held in his name with an address of 2 Bodell Ave, Apt 6, Providence, RI 02909. Chase Bank closed account #XXXXXX3608 on March 27, 2020 and account #XXXXX3426 on March 30, 2020 respectively.

87. A review of activity on the account revealed on March 18, 2020, United States Treasury check #XXXX7533 in the amount of $5,292.00 made payable to JK and dated March 13, 2020, was deposited into Chase Bank Account #XXXXX3426. On the back of the check

was the alleged signature of JK followed by the signature of what appears to be Richard KOBOI. The deposit was made via an ATM transaction at the Chase Bank branch located at 869 Providence Highway, Dedham, MA. Chase Bank restricted this deposit due to the presence of a third-party payee and was unable to verify issuance of the item from JK.

88. On December 29, 2020, I spoke with JK regarding the United States Treasury check in question. JK stated she was aware that her check was stolen because she received a letter from Chase Bank regarding her knowledge of the transaction. JK stated she has also contacted the IRS regarding the stolen check and requested a new check be issued, which she has yet to receive. JK stated she moved in February 2020 and wasn't even at the address where the check was mailed. USPS records show that a change of address form (PS 3575) was submitted in-person by JK on March 5, 2020, requesting an address change 152 Massachusetts Ave, Providence, RI (the address which was listed on her Treasury check) to 539 Dexter St., Apt. A, Providence, RI. Notably, 539 Dexter St, Apt. B, Providence, RI is the address for KOBOI's mother.[23] JK stated she has never heard of Richard KOBOI and that the signature on the back of the check was not her handwriting. KOBOI's Facebook records under "Sunnyboy Taylor" show that he conducted searches on Facebook for JK's full name on March 18, 2020.

ADDITIONAL ACTIVITY INVOLVING KOBOI

89. On December 3, 2020, I was notified by Detective Chea of the Warwick (RI) Police Department regarding a counterfeit check that was deposited into a Pawtucket CU account. Det. Chea stated that the Pawtucket CU bank manager reported a fraudulent check for $8,200.00 was deposited on October 16, 2020 at the Pawtucket CU ATM located at 405 Warwick, Ave, Warwick, RI. Subsequently, between October 20-21, 2020, there were two ATM cash withdrawals and two point of sale withdrawals via the Apple Cash app.

90. A Pawtucket CU bank investigator contacted the payor of the check, The Law Office of Robert V. Russo, who confirmed that the check was indeed fraudulent. Additionally, the

[23] Rhode Island Department of Corrections records revealed KOBOI listed his mother as Louise Taylor. Rhode Island DMV records show Louise Taylor's driver's license was issued on March 29, 2019, and lists her address as 539 Dexter St, Apt B, Providence.

Pawtucket CU bank investigator contacted the payee of the check, Darren Maenza, in an effort to recover the funds but was unable to get in contact with him.

91. Surveillance photographs provided by Pawtucket CU show KOBOI making the aforementioned deposit at the Pawtucket CU ATM located at 405 Warwick Ave, Warwick, RI on October 16, 2020 at 6:42 PM. Additionally, a silver chain and padlock pendant worn by KOBOI in one of the surveillance photos is identical to a silver chain and padlock pendant he is wearing in several photos on his Facebook page.

92. Facebook records for "Sunnyboy Taylor" revealed on October 20, 2020 a bank account screenshot with the name "DARREN MAENZA" and current balance of $8,381.36 was sent by "Sunnyboy Taylor" to "Sos DMann". This photo appears to be related to the counterfeit check deposit referenced in paragraph 86.

93. Facebook records for "Sunnyboy Taylor", revealed a conversation between "Sos DMann" and "Sunnyboy Taylor" that took place on October 19, 2020. Below is part of the conversation discussing depositing a counterfeit check:

> *Sos DMann: Yo bro do first citizens work? I gotta go to New Bedford to grab an don't wanna waiste time if not gone hit*
> *Sunnyboy Taylor: definitely*
> *Sunnyboy Taylor: online drop*
> *Sunnyboy Taylor: will pop for us off top*
> *Sos DMann: Bet say dat*
> *Sunnyboy Taylor: trust me*
> *Sunnyboy Taylor: go grab it*
> *Sos DMann: Wait she said she only got card*
> *Sunnyboy Taylor: that's cool*
> *Sunnyboy Taylor: we can drop it out there*
> *Sos DMann: Bet*
> *Sunnyboy Taylor: got that card for you too*
> *Sos DMann: Oh yeah thank u bro she's going nuts I'm be done in a hr*
> *Sunnyboy Taylor: lmk , got you*
> *Sos DMann: Jason J Rose - first citizen*

94. Furthermore, on October 21, 2020, "Sunnyboy Taylor" messages "Sos DMann" a photo of a First Citizens Federal Credit Union (FCU) receipt showing a check from the Law Office of Robert V. Russo made payable to Jason J. Rose in the amount of $9,637.02. The receipt displays a deposit date of October 20, 2020 at 20:47 hours.

95. On January 7, 2021, I spoke with First Citizens FCU bank investigator Susan Oliveira who confirmed a fraudulent check for $9,637.02 was deposited on October 20, 2020 at

the First Citizens FCU ATM located at 629 South St West, Raynham, MA. Subsequently, on October 23, 2020, there were four ATM cash withdrawals totaling $9,601.00 and two point of sale withdrawals before the check was ultimately deemed fraudulent.

96. Surveillance photographs provided by First Citizens FCU show KOBOI making the aforementioned deposit at the First Citizens FCU ATM located at 629 South St West, Raynham, MA on October 20, 2020 at 20:46 hours.

97. Using law enforcement databases and open social media pages, we were able to identify "Sos DMann" as Dante Mann of Providence, RI. Mann was murdered on October 22, 2020 on Gallup St in Providence while filming a music video.

SUBJECT PREMISES 1: 211 HANOVER ST, APT. 1, PROVIDENCE, RI

98. A mail cover for 211 Hanover St., Apt. 1, Providence, RI, revealed between June 23, 2020 and July 22, 2020, Patrick JOHNSON and Patricia JOHNSON received mail at 211 Hanover St, Floor/Unit 1, Providence, RI to include a Cox Communications invoice and a Verizon invoice. The address listed is the SUBJECT PREMISES 1. An additional mail cover for 211 Hanover St., Apt 1, Providence, RI, revealed between February 2, 2021 and February 18, 2021, Patrick JOHNSON and Patricia JOHNSON continued to receive mail, including a credit card and E-Z Pass invoice, at the SUBJECT PREMISES 1.

99. A search of the USPS Change of Address system revealed as of February 18, 2021, no change of address requests were submitted that listed 211 Hanover St., Apt 1, Providence, RI as a previous address. Furthermore, on August 22, 2019, Patrick JOHNSON submitted a change of address request through the USPS, requesting his address be changed from 40 Sterling Ave, Providence, RI to 211 Hanover St, #1, Providence, RI.

100. Rhode Island DMV records for both Patricia JOHNSON and Whayee Sarkpah-Johnson list 211 Hanover St., Providence, RI as their address.

101. Further, Patricia JOHNSON Citizen's Bank Account #XXXXXX0873, used to deposit a counterfeit check, lists an address of 211 Hanover St, Apt 1, Providence, RI 02907. Funds from a counterfeit HELOC check deposited in Individual #1's TD Bank account were used to purchase two money orders made payable to Patricia JOHNSON, 211 Hanover, Prov, RI. In addition, the December 23, 2019, mailing of counterfeit HELOC checks by

Patrick JOHNSON was paid for with a debit card issued to Whayee Sarkpah-Johnson of 211 Hanover Street, Providence, RI.

102. On multiple occasions on September 8, 2020, an individual believed to be Patricia JOHNSON was observed exiting and entering the SUBJECT PREMISES 1 in a vehicle registered to her. On September 8, 2020 at approximately 6:44 AM, a 2013 red Kia Optima bearing RI registration SR561 departed the SUBJECT PREMISES 1 driven by an unknown short black female with reddish hair. RI registration SR561 is registered to a 2013 red Kia Optima in the name of Patricia F. JOHNSON at 211 Hanover Street, Apt 1, Providence, RI. Continuing on the same date, at approximately 6:54 AM, the red Kia Optima bearing RI registration SR561 returned to the SUBJECT PREMISES driven by the unknown short black female with reddish hair.

103. The fraudulent credit card application described in paragraph 48 above which identified Patrick JOHNSON as an authorized user, listed a mailing address of 211 Hanover St, Providence, RI. Based on my experience, once a credit card application is approved, the credit card company will send the newly issued credit card to the address that the applicant designates. Accordingly, individuals involved in credit card fraud will use an address where they can receive the credit card after the fraudulent credit card is issued by the bank.

SUBJECT PREMISES 2: 439 ADMIRAL ST, APT 3, PROVIDENCE, RI

104. Facebook records provided the following information for username “Teebone Juheard”, the Facebook account associated with RICHARDSON. Facebook records revealed on August 23, 2020 at 21:02 UTC, RICHARDSON logged into his Facebook account from IP 100.40.76.71. Records provided by Verizon revealed IP 100.40.76.71 is associated with Electra Smith with the address listed as the SUBJECT PREMISES 2. Additionally, Facebook records for “Teebone Juheard” show conversations with “Lectra Smith” in which “Lectra Smith” refers to “Teebone Juheard” as the father of their child.

105. In a Facebook message from Lectra Smith to Teebone Juheard on April 30, 2020, at approximately 7:50 p.m. Smith states, “Just got home.” Smith then asks, “Wyd” believed to be short for “What are you doing?” RICHARDSON using the Teebone Juheard account responds, “Checks.” At approximately 11:40 p.m. and 12:03 a.m. that same

night, Smith sends Facebook messages to RICHARDSON of photographs of a what appears to be a phone (one photograph displays a finger holding the phone) that contained the following messages from another individual identified by first name only, "I work in Newport though it's a drive[.] If you can make it tomorrow between 10-3 I have another teller on with me who will be doing transactions i can make it work[.] She'll have to ask me for approval but that's easy[.]" and "An account usually has to be at least 3 months old to not throw up any red flags for large deposits."

106. On Tuesday, December 1, 2020, RICHARDSON was observed by law enforcement surveillance arriving at the Garrahy Judicial Complex for a meeting with his probation officer. RICHARDSON arrived for his meeting in the blue Ford Fusion with Rhode Island tag FQ861. A query of FQ861 (RI) revealed it was registered to Enterprise Rent-A-Car located at 1674 Hartford Ave. in Johnston, RI. Enterprise records show that the Ford Fusion was rented to Electra Smith with the address listed as the SUBJECT PREMISES 2. That vehicle was observed parked at the SUBJECT PREMISES 2 by law enforcement on both December 1-2, 2020.

107. On December 8, 2020, the Honorable Patricia A. Sullivan signed a search warrant (20-SW-441-PAS), authorizing the search of T-Mobile records for RICHARDSON (Mobile # 401-677-9165), TARGET PHONE #1, including information about the location of the cellular telephone number.

108. On December 18, 2020, between 5:12 AM PST – 8:12 AM PST, location alerts for TARGET PHONE #1 revealed that the phone in question was in the area of the SUBJECT PREMISES 2 as detailed below:

DATE	TIME (PST)	LATITUDE	LONGITUDE	UNCERTAINTY
12/18/2020	5:12:26 AM	41.846613	-71.429844	88m
12/18/2020	5:42:26 AM	41.846613	-71.429844	88m
12/18/2020	5:57:26 AM	41.846613	-71.429844	88m
12/18/2020	6:27:26 AM	41.846613	-71.429844	88m
12/18/2020	6:42:27 AM	41.846613	-71.429844	88m
12/18/2020	6:57:32 AM	41.846613	-71.429844	88m
12/18/2020	8:12:26 AM	41.846613	-71.429844	88m

109. Between December 26, 2020 at 9:57 PM PST and December 27, 2020 at 12:12 PM PST, location alerts for TARGET PHONE #1 revealed that the phone in question was mostly in the area of the SUBJECT PREMISES 2 as detailed below:

DATE	TIME (PST)	LATITUDE	LONGITUDE	UNCERTAINTY
12/26/2020	9:57:31 PM	41.846613	-71.429844	88m
12/26/2020	10:27:31 PM	41.846613	-71.429844	88m
12/26/2020	10:42:32 PM	41.846613	-71.429844	88m
12/26/2020	11:12:27 PM	41.846613	-71.429844	88m
12/26/2020	11:42:29 PM	41.846613	-71.429844	88m
12/27/2020	12:27:28 AM	41.846613	-71.429844	88m
12/27/2020	12:42:27 AM	41.846613	-71.429844	88m
12/27/2020	12:57:29 AM	41.846613	-71.429844	88m
12/27/2020	1:12:27 AM	41.846613	-71.429844	88m
12/27/2020	1:27:28 AM	41.846613	-71.429844	88m
12/27/2020	1:42:25 AM	41.846613	-71.429844	88m
12/27/2020	1:57:29 AM	41.846613	-71.429844	88m
12/27/2020	2:12:26 AM	41.846613	-71.429844	88m
12/27/2020	2:27:26 AM	41.846613	-71.429844	88m

110. On February 17, 2021, between 1:40 AM PST – 11:10 AM PST, location alerts for TARGET PHONE #1 revealed that the phone in question was in the area of the SUBJECT PREMISES 2 as detailed below:

DATE	TIME (PST)	LATITUDE	LONGITUDE	UNCERTAINTY
2/17/2021	1:40:54 AM	41.846613	-71.429844	88m
2/17/2021	2:25:55 AM	41.846613	-71.429844	88m
2/17/2021	3:25:56 AM	41.846613	-71.429844	88m
2/17/2021	4:25:56 AM	41.846613	-71.429844	88m
2/17/2021	5:25:55 AM	41.846613	-71.429844	88m
2/17/2021	6:10:55 AM	41.846613	-71.429844	88m
2/17/2021	8:40:57 AM	41.846613	-71.429844	88m
2/17/2021	9:25:55 AM	41.846613	-71.429844	88m
2/17/2021	10:25:57 AM	41.846613	-71.429844	88m
2/17/2021	11:10:55 AM	41.846613	-71.429844	88m

111. On December 30, 2020, the USPS North Station delivery unit confirmed Electra Smith and Jennifer Creighton are currently receiving mail at the SUBJECT PREMISES 2.

112. A mail cover for 439 Admiral St., 3rd Floor, Providence, RI, confirmed between February 2, 2021 and February 18, 2021, Electra Smith received mail at the SUBJECT PREMISES 2 to include a Progressive Insurance documents.

113. A search of the USPS Change of Address system revealed as of February 18, 2021, no change of address requests were submitted that listed 439 Admiral St., Providence, RI as a previous address. Furthermore, on April 27, 2020, Jennifer Creighton submitted a change of address request through the USPS, requesting her address be changed from an address in Central Falls, RI to the SUBJECT PREMISES 2.

SUBJECT PREMISES 3 RENTED AND USED BY KOBOI, TARGET PHONE #2 USED BY KOBOI, TARGET VEHICLE RENTED AND USED BY KOBOI

114. On January 29, 2021, the Honorable Patricia A. Sullivan signed a search warrant (21-SW-017-PAS), for TARGET PHONE #2 used by KOBOI for prospective location information.

115. On February 10, 2021, agents from the US Secret Service assisted with conducting surveillance of KOBOI. Ping locations for KOBOI between 3:38 AM and 4:53 AM showed KOBOI in the area of Gloucester Street (Lat: 41.850829, Long: -71.437376) in Providence, RI with 88m of uncertainty. While canvassing the surrounding areas, Agents came across the TARGET VEHICLE, a silver Chevrolet Colorado bearing CA registration 37035X2 across the street from 754 River Ave in Providence, RI. An NCIC query of this vehicle revealed it was registered to Hertz Vehicles, LLC out of Los Angeles, CA.

116. Continuing on February 10, 2021, I contacted the security department at Hertz regarding the TARGET VEHICLE. An investigator with Hertz confirmed that this vehicle was rented to Richard KOBOI of 2 Bodell Ave in Providence, RI. The investigator stated that KOBOI provided a Rhode Island driver's license (3319453[24]) and a phone number of (267) 854-9972, TARGET PHONE #2, to acquire the rental vehicle. The investigator stated the TARGET VEHICLE was rented on February 4, 2021 from Dollar Rent-A-Car[25] at TF Green Airport and was initially due to be returned on February 7, 2021. The investigator stated the rental return date was extended by KOBOI but due to the credit card used to extend the rental being declined, the TARGET VEHICLE was now due back on February 12, 2021.[26]

---

[24] According to RI DMV records, RI driver's license #3319453 is associated with Richard KOBOI, 2 Bodell Ave, Apt 6, Providence, RI 02909.

[25] Dollar Rent-A-Car operates as a subsidiary of the Hertz Corporation.

[26] A prior traffic stop of Richard KOBOI on January 8, 2021, by the Rhode Island State Police (RISP) showed that he was driving a different rental vehicle with tinted windows rented to Pamela Halloway and returned on January 20, 2021. During the traffic stop, the citation report indicates that "a few grand ditched in the door upon exit." On February 23, 2021, I spoke with the RISP Trooper Corey Hopkins who made the traffic stop. The Trooper indicated that when KOBOI exited the vehicle, he removed from his pockets and placed what appeared to be few

117. On February 12, 2021, ping locations for KOBOI between 12:23 PM and 12:38 PM showed KOBOI in the area of Smithfield Ave (Lat: 41.8593254, Long: -71.411133) in Pawtucket, RI with 88m of uncertainty. While canvassing the surrounding areas, Inspectors came across the TARGET VEHICLE outside 210 Seneca Ave in Pawtucket, RI. This is the same address KOBOI provided to an individual during their Facebook conversation. The TARGET VEHICLE appeared to have aftermarket tinted windows, which based upon my experience assists fraudsters and felons with concealing their criminal activity, proceeds of the crime, and weapons.

118. On February 16, 2021, I spoke to an investigator with Hertz who stated that KOBOI never returned the rental car on February 12, 2021 and that the TARGET VEHICLE was now due to be returned on February 17, 2021.

119. On February 16, 2021, the Honorable Lincoln D. Almond signed a search warrant (21-SW-046-LDA), authorizing the installation of a vehicle tracking device on a 2020 Chevrolet Colorado, the TARGET VEHICLE currently being rented by KOBOI. That tracking device was successfully installed by Postal Inspectors on the morning of February 17, 2021.

120. Between February 18, 2021 and February 24, 2021, data from the tracking device revealed the TARGET VEHICLE pinging numerous times in a parking lot behind the 91 Loft Apartments located at 91 Hartford Ave, Providence, RI, which is SUBJECT PREMISE 3, showing that it stopped and rested there overnight on multiple days. Notably, the vehicle tracker has the accuracy of 1 meter.

121. On February 22, 2021, around 8:00 p.m. the tracking device showed the TARGET VEHICLE at the First Citizens Bank in New Bedford, Massachusetts. An ATM surveillance photo obtained from First Citizens Bank showed what appears to be an image of an unidentified male, not KOBOI, in the back seat of the driver side attempting to make a transaction. Subsequently, the tracking device showed that the TARGET VEHICLE went to a Stop and Shop on Branch Avenue in Providence and then to the parking lot of SUBJECT PREMISE 3 at approximately 11:27 a.m. Based upon my experience,

---

thousand dollars in the car door compartment. Also in the vehicle was a female passenger. The Trooper stated that the money was bundled up in multiple denominations. KOBOI stated to the Trooper that it was his girl's money.

individuals engaging in bank/wire fraud will use their vehicles to travel to banks to make deposits of counterfeit checks and/or withdrawals when the funds of the counterfeit checks become available.

122. On February 23, 2021, at approximately 3:20 p.m. I observed the TARGET VEHICLE in the parking lot of SUBJECT PREMISE 3. On February 24, 2021, United States Secret Service agents assisting in the investigation observed the TARGET VEHICLE in the parking lot of the SUBJECT PREMISE 3 at approximately 7:34 a.m. On the same date, I observed the TARGET VEHICLE in the parking lot of the SUBJECT PREMISE 3 from approximately 10:30 a.m. - 1:30 p.m.

123. On February 24, 2021, I spoke to the leasing manager at the 91 Lofts Apartment who provided me with records confirming KOBOI signed a one year lease agreement using the name "Sunnyboy Richard Koboi" for the SUBJECT PREMISE 3 on January 15, 2021. KOBOI then moved into Apartment 131, a studio apartment, on February 1, 2021, the start date for the lease. The leasing manager stated KOBOI provided a RI driver's license as identification, a phone number of 267-854-9972, which is TARGET PHONE #2, and an email address of richardkoboi95@gmail.com.

124. The leasing manager stated that KOBOI lives by himself and that there are no other occupants listed on the lease. Both the security deposit of $1500 and first month of rent of $1500 that was due upon signing the lease was paid for in cash.

125. While at the SUBJECT PREMISE 3, I viewed video surveillance footage from multiple cameras all around the apartment complex for February 22, 2021, at 11:27 p.m., the same time the TARGET VEHICLE was pinging in the parking lot of the SUBJECT PREMISES 3. KOBOI was observed on camera entering the complex parking lot in the TARGET VEHICLE. After parking, KOBOI met up with two other individuals who arrived in a separate vehicle and parked directly in front of KOBOI. After a short conversation in the parking lot, KOBOI and the two individuals, entered a side entrance and video surveillance showed that KOBOI entered Apartment 131. It should be noted that access to the apartment building is with a key fob and unique access code. Records related to key fob activity by KOBOI were requested and are currently being prepared by a 3rd party company that maintains the information.

126. Based upon my review of the tracking device pings of the TARGET VEHICLE at the SUBJECT PREMISE 3, cell phone location for TARGET PHONE #2 being in the vicinity of the SUBJECT PREMISE 3, discussions with the leasing manager for SUBJECT PREMISE 3, review of leasing records for SUBJECT PREMISE 3, and review of video surveillance from TARGET PREMISE 3 which shows KOBOI entering TARGET PREMISE 3, I believe TARGET PREMISE 3 is KOBOI's current residence.

E. SUMMARY OF DEFENDANTS INVOLVEMENT

127. As described herein, from November through December 2019, Patrick JOHNSON mailed out at least seven counterfeit HELOC checks totaling $384,700 to various individuals throughout the United States for them to deposit and withdraw the funds**.** Based upon my training and experience, JOHNSON was assisted by other co-conspirators in the scheme as he appears to be talking and/or texting and/or taking photos on a cellphone while conducting some of these mailing transactions inside the post office as shown by post office video surveillance which captured JOHNSON. In addition, JOHNSON taking photographs of the mailing envelopes suggests that he and/or a co-conspirator intended to follow up with the counterfeit check recipient in order to obtain the funds deposited.

128. As described herein, in October of 2019, Individual #1 received a counterfeit Beth Page FCU HELOC check from Patrick JOHNSON and was instructed to deposit it into her TD Bank account. Patrick JOHNSON, accompanied by Terrance RICHARDSON and Individual #1's boyfriend at the time, then drove Individual #1 to the USPS Post Office and instructed her to purchase money orders. Those money orders were made payable to and cashed the following day by Patricia JOHNSON whose driver's license number was recorded as identification presented for the transaction.

129. As described herein, in October of 2019, a fraudulent credit card application in the name DB was submitted online to US Bank using DB's social security number and date of birth. The application identified Patrick JOHNSON as an authorized user and listed a mailing address of 211 Hanover St, Providence, RI. Additionally, records related to the email address Fainb659@gmail.com that was used on the application listed a recovery telephone number of (347) 230-7119. That number is associated with a MagicJack account that lists an address of 211 Hanover St, Apt 2, Providence, RI.

130. As described herein, on January 23, 2020, KOBOI and Patricia JOHNSON conversed over Facebook messenger about using her Citizen's Bank account to deposit a counterfeit check into and then to withdraw those funds. In the Facebook conversation, KOBOI made arrangements to pick up Patricia JOHNSON's bank card outside SUBJECT PREMISES 1, and Patricia JOHNSON provided KOBOI her online banking login and password as well as her bank card pin. As described herein, on January 23, 2020, a check for $8,352.16, made payable to Patricia JOHNSON was deposited into her Citizens Bank account via an ATM deposit. Prior to the check being returned as fraudulent, approximately $4,500.00 of the funds from the account were removed via ATM withdrawals and debit card purchases.

131. As described herein, Facebook records pursuant to a federal search warrant for account "Teebone Juheard" revealed that Terrance RICHARDSON communicated with various co-conspirators to cash/deposit counterfeit checks, obtain information for cashing/depositing counterfeit checks, and/or produce paper stock for counterfeit checks. Among the counterfeit checks that RICHARDSON caused to be deposited was in Individual #5's name and using Individual #5's debit card information. RICHARDSON then refused to return Individual's #5 debit card back to him and sent a photograph of the debit card next to what appears to be handgun.

132. As described herein, between April 14, 2020 and July 9, 2020, six checks totaling $115,877.69, made payable to Terrance RICHARDSON were deposited into his Chase Bank accounts via ATM deposits. Prior to the checks being returned as fraudulent, RICHARDSON was able to obtain approximately $42,547.66 of the funds from the accounts via debit card transactions, ATM withdrawals and money transfers to various bank accounts. Surveillance photographs and video provided by Chase Bank show RICHARDSON making several of the aforementioned cash withdrawals and wearing a gold chain with a "TEE BONE" diamond pendant in some of the surveillance photos which is identical to the gold chain and diamond pendant he is wearing in several photos on his Facebook page "Teebone Juheard."

133. As described herein, Facebook records obtained pursuant to a federal search warrant for account "Sunnyboy Taylor" revealed that KOBOI communicated with various co-conspirators to cash/deposit counterfeit checks, obtain information for cashing/depositing counterfeit checks, and for creating fraudulent checks.

134. As described herein, KOBOI's Facebook messages with a co-conspirator showed that KOBOI caused a counterfeit check drawn on victims MB and DB's HELOC bank account to be deposited into that co-conspirator's Citizens Bank account on November 4, 2020. DB was the identity theft victim associated with the fraudulent credit card application submitted in DB's name on October 28, 2019, in which Patrick JOHNSON was identified as an authorized user.

135. As described herein, between April 8, 2020 and April 9, 2020, three checks totaling $14,494.20, made payable to Richard KOBOI were deposited into his Wells Fargo accounts via ATM deposits. Prior to the checks being returned as fraudulent, KOBOI was able to obtain approximately $9,131.19 of the funds from the accounts via ATM withdrawals and debit card purchases. Surveillance photographs provided by Wells Fargo show KOBOI making the aforementioned deposits in Delaware and Connecticut, and one of the subsequent withdrawals in Connecticut. Additionally, a gold chain worn by KOBOI in one of the surveillance photos is identical to a gold chain he is wearing in several photos on his Facebook page.

136. As described herein, on March 18, 2020, a US Treasury check for $5,292.00, made payable to victim JK was deposited into KOBOI's Chase Bank account via an ATM deposit. Ultimately, Chase Bank restricted this deposit due to the presence of a third-party payee. The victim confirmed it was stolen, negotiated without her consent, and that the endorsement on the check was not JK's signature.

137. As described herein, between July 6, 2020 and July 30, 2020, Richard KOBOI received six ACH credits into his Bank Newport account, totaling $5,685.00, from three different state sponsored entities which were ultimately deemed fraudulent.

138. As described herein, I was notified by the Warwick (RI) Police Department regarding a counterfeit check that was deposited via ATM into a Pawtucket Credit Union account on October 16, 2020. Surveillance photographs provided by Pawtucket CU show Richard KOBOI making the aforementioned deposit at the Pawtucket CU ATM.

139. As described herein, after reviewing records related to KOBOI's Facebook account, a bank investigator with First Citizens FCU confirmed a counterfeit check was deposited via ATM into a First Citizens FCU account on October 20, 2020. Surveillance

photographs provided by First Citizens FCU show Richard KOBOI making the aforementioned deposit at the First Citizens FCU ATM.

TRAINING AND EXPERIENCE ON FRAUD AND FIREARM OFFENSES

140. Based on my training and experience and familiarity with investigations into fraud conducted by other law enforcement agents, I know the following:

a. Individuals maintain in their homes and vehicles, both in paper and electronic format, among other items, records regarding the receipt and expenditure of money, documents relating to the purchase of assets, and records pertaining to their employment or business. Similarly, given the nature of the fraud, based on my training and experience, I believe that participants in a long running fraud that involves several participants, more often than not, will keep records containing names, addresses, email addresses, and telephone numbers of co-conspirators, as well as targets and victims, amounts received from them, and amounts sent to co-conspirators. These records are necessary to further the illicit fraud business and can be found in paper form or stored electronically in cell phones and other electronic devices. Owing to the long-term usefulness of such items, and tracking relative proceeds among co-conspirators, this type of evidence would likely be generated, maintained, and then possibly forgotten about and not disposed of.

b. There are many reasons why criminal offenders maintain evidence for long periods of time. First, to the offender, the evidence may seem innocuous at first glance (e.g. financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, checkbooks, videotapes and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone and pager bills, keys to safe deposit boxes, packaging materials, computer hardware and software). To law enforcement, however, such items may have significance and relevance when considered in light of other evidence. Second, the criminal offender may no longer realize he/she still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that he/she has deleted, hidden or further destroyed computer-related evidence,

which in fact, may be retrievable by a trained forensic computer expert. Thus, records and ledger-type evidence that one would think a prudent person might destroy because of its incriminatory nature are sometimes still possessed months or even years after the records were created.

c. From training and experience I know that individuals who amass proceeds from illegal activities routinely attempt to further that conduct and/or conceal the existence and source of their funds by engaging in financial transactions with domestic and foreign institutions, and others, through all manner of financial instruments, including cash, cashier's checks, money drafts, traveler's checks, wire transfers, etc. Records of such instruments are oftentimes maintained at the individual's residence or some other place over which they maintain dominion and control.

d. In addition, during the course of such residential searches, I and other agents have also found items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the SUBJECT PREMISES and computer devices located therein. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys.

e. Based on my experience and the experience of Alcohol, Tobacco, Firearms, and Explosives (ATF) agents who have assisted me in this investigation, persons prohibited from possessing firearms keep their firearms in locations for safekeeping and which they can access to include their residences, residences of close associates, and vehicles. They do so in order to protect the proceeds of their criminal activity and because of the value of the firearms and the difficulty in obtaining such firearms as prohibited persons.

TRAINING AND EXPERIENCE ON DIGITAL DEVICES[27]

[27] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives;

141. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices

---

related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

142. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

143. Because several people may share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

144. The search warrant also requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature

matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress TERRANCE RICHARDSON/ RICHARD KOBOI/ PATRICK JOHNSON's/PATRICIA JOHNSON's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of RICHARDSON/KOBOI/ PATRICK JOHNSON/PATRICIA JOHNSON's face with his/her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

d. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

BACKGROUND ON T-MOBILE AND E-911

145. Based upon my training and experience, I believe that the E-911 Phase II data provided by T-Mobile will be of benefit in locating the movements of the individual utilizing the TARGET PHONES 1-2 and this locator information provided will be of benefit in identifying the location and or locations that RICHARDSON and KOBOI are utilizing to deposit fraudulently obtained funds; the locations RICHARDSON and KOBOI are using to meet with co-conspirators, and the locations to possibly include the physical residences of any other criminal co-conspirators involved in this counterfeit check cashing scheme; and the identification of locations where proceeds and facilitating property used in the bank fraud scheme are stored including but not limited to printers, check stock, and victims' bank information to include debit cards.

146. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate at least two kinds of information about the locations of the cellular telephones to which they provide service: (1) E-911 Phase II data, also known as GPS data or latitude-longitude data, and (2) cell-site data, also known as "tower/face information" or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data.

147. Based on my training and experience, I know that T-Mobile can collect E-911 Phase II data about the location of the TARGET PHONES including by initiating a signal to determine the location of the TARGET PHONES on T-Mobile's network or with such other reference points as may be reasonably available. Additionally, I know that T-Mobile can collect cell-site data about the TARGET PHONES.

IV. CONCLUSION

148. From my training and experience, I am aware that the counterfeit check scheme described above is extremely widespread. According to records maintained by the Postal Inspection Service, this scheme and similar schemes have affected thousands of victims in the United States. These victims reside throughout the United States. In my training and experience and based upon my review of the records in this case, it is likely that the same individuals who victimized the aforementioned individuals have victimized other individuals using the same or similar scheme. In my training and experience, fraudsters using these

counterfeit check cashing techniques tend to follow the same *modus operandi* in their interactions with different victims.

149. Based upon my experience and my knowledge of these types of scams and social media postings, there is probable cause to believe that Terrance RICHARDSON, Richard KOBOI, and Patrick JOHNSON were engaged in a counterfeit check kiting / cashing schemes in violation of in violation of 18 U.S.C. § 1344 (Bank Fraud), in violation of 18 U.S.C. § 1343 (Wire Fraud), in violation of 18 U.S.C. § 1349 (Conspiracy to Commit Wire and Bank Fraud), and 18 U.S.C. § 1028A (Aggravated Identity Theft). From the Facebook records that I have reviewed thus far, including interviews conducted, the schemes are as follows:

   a. RICHARDSON and KOBOI recruit individuals who have a bank account or are willing to establish a bank account at their request. Based on their Facebook postings it appears that RICHARDSON and KOBOI prefer individuals who already have a bank account established.[28] One of the individuals recruited by KOBOI was Patricia JOHNSON who provided KOBOI with her bank account information and bank card to deposit a counterfeit check.
   b. RICHARDSON, KOBOI, and/or Patrick JOHNSON then request that the individual provide to them his/her identification and his/her bank card and/or accompany the individual to the bank to make the counterfeit check deposit. I believe that RICHARDSON and KOBOI often keep that individual's identification as collateral and then establishes (or has the co-conspirator establish) a mobile banking relationship with their bank. This permits the co-conspirator, RICHARDSON, and/or KOBOI to perform activities such as a mobile deposit.[29]

[28] Based upon my training and experience including dozens of investigations involving the banking system while employed with the United States Secret Service, I am aware that individuals using the banking system to commit fraud often prefer established bank accounts over newly created accounts because the banks often utilize more rigorous fraud mechanisms against newly created accounts. This enables an established account holder to have the ability to defraud a bank of more money than a newly created account would be able to do.

[29] A mobile deposit is a feature commonly offered by banks whereby they allow a user to take a picture of a negotiable instrument such as a check or money order and deposit the item into their bank account without ever visiting the bank.

c. RICHARDSON and KOBOI offer to compensate the co-conspirator in varying amounts based on the type of account the individual has at their respective bank.

d. Based on the various bank policies (which appears to be how RICHARDSON associates a value to the account), the bank will often allow a percentage of the deposited funds to show as available pending the clearing of the full amount. Often times these funds are shown as available immediately after the negotiable instrument is deposited into the account via the mobile banking application.

e. Using these available funds, RICHARDSON, KOBOI, and/or a co-conspirator then visit a bank branch and utilize the debit card and PIN number to remove the available funds from the account and/or transfer funds online. However, some banks limit the amount of cash that can be immediately withdrawn but will allow the funds to be used for other purchases.

f. Several days later, once the negotiable instrument is returned to the bank as fraudulent, the bank attempts to restrict the account and make contact with the account holder. The bank will advise the account holder that they can either repay the amount or they will be sent to collections. If the amount remains uncollectible the bank may submit the claim to their insurance provider for coverage on the loss.

g. In addition, Patrick JOHNSON and possibly others unknown to investigators at this time mailed out counterfeit check to individuals throughout the country in this mail/bank/wire fraud scheme. While it is unclear at this time on how these individuals receiving the checks were targeted and how JOHNSON and/or his co-conspirators were to obtain the funds from these counterfeit check deposits, there is probable cause to believe that the search of SUBJECT PREMISES 1 will contain evidence of the mail/bank/wire fraud scheme and conspiracy given the expansive scope of this interstate scheme.

h. Further in this fraud scheme, Terrance RICHARDSON used the name of a real individual on a counterfeit check and the real individual's debit card information to deposit a counterfeit check into that individual's bank account, Richard KOBOI used the name and forged signature of real individual in an attempt to deposit a U.S. Treasury check into KOBOI's own bank account, and Patrick JOHNSON

also used the name and identifying information of a real individual in a credit application in an attempt to fraudulently obtain a credit card in the victim's name.

150. Based on all of the foregoing facts, I submit that there is probable cause search the SUBJECT PREMISES, TARGET PHONES, and TARGET VEHICLE for the items described in the corresponding attachments attached to this affidavit and referenced in paragraph 2.

151. Based on the foregoing, I also request that the Court issue the proposed search warrants for information about the location of TARGET PHONES #1 and #2, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c). I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the TARGET PHONES #1 and #2 would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. See 18 U.S.C. § 3103a (b)(l). It is further requested that the Court ORDER T-Mobile not to disclose the existence of the warrant sought even if the customer should inquire as to the existence of any tracking warrants. As further specified in Attachment D, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. See 18 U.S.C. § 3103a (b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. See 18 U.S.C. § 3103a (b)(2).

152. I further request that the Court direct T-Mobile to disclose to the government any information described in Attachment D that is within the possession, custody, or control of T- Mobile. I also request that the Court direct T-Mobile to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment D unobtrusively and with a minimum of interference with T-Mobile' s services, including by initiating a signal to determine the

location of the TARGET PHONES #1 and #2 on T- Mobile's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate T- Mobile for reasonable expenses incurred in furnishing such facilities or assistance.

153. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the TARGET PHONES #1 and #2 outside of daytime hours.

154. Because this investigation is continuing and disclosure of some of the details of this affidavit may cause the targets or other affiliated persons to flee or further mask their identity or activities, destroy physical and/or electronic evidence, or otherwise obstruct and seriously jeopardize this investigation, I respectfully request that this affidavit, and associated materials seeking this search warrant, be sealed for a period of 90 days or until further order of this Court. Finally, I specifically request that the sealing order not prohibit information obtained from this warrant from being shared with other law enforcement and intelligence agencies.

I declare that the foregoing is true and correct.

Cory P. McManus
Postal Inspector
US Postal Inspection Service

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by **Sworn telephonically and signed electronically**.
(*specify reliable electronic means*)

February 26, 2021	
Date	*Judge's signature*
Providence, Rhode Island	**Patricia A. Sullivan, USMJ**
City and State	*Printed name and title*

ATTACHMENT A-1

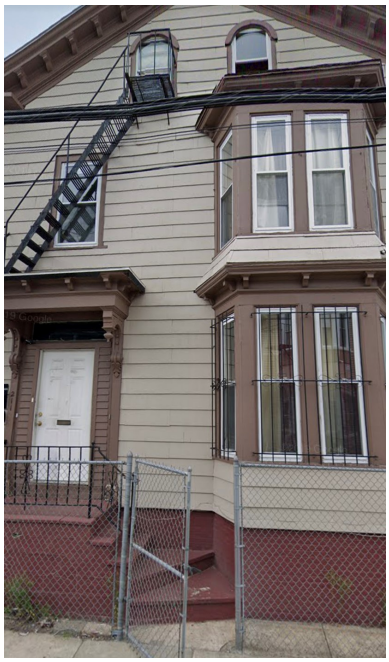
PREMISES TO BE SEARCHED

The SUBJECT PREMISES 1 is the premises at 211 Hanover Street, Apt 1, Providence, RI 02907. SUBJECT PREMISES 1 is described as a multi-family home. SUBJECT PREMISES 1 is the 3rd multi-family home on the left, in a group of six similarly-styled multi-family homes on Hanover Street. The numbers "211" is clearly marked in black numbers to the left of the front door.

The area to be searched at the SUBJECT PREMISES 1 includes all rooms, annexes, attics, basements, porches, garages, carports, outside yard area, curtilage, mailboxes, trash containers, debris boxes, storage lockers, locked containers and safes, lockers, sheds, and any visible structures and outbuildings associated with the SUBJECT PREMISES 1 and shall extend into desks, cabinets, safes, briefcases, backpacks, wallets, purses, digital devices, and any other storage locations within SUBJECT PREMISES 1.

The search shall also include any computers, cellular telephones, storage media/medium, and digital devices.

The search shall also include any person located at the SUBJECT PREMISES 1, as defined above, at the time the search warrant is executed, and any computers, cellular telephones, storage media/medium, briefcases, backpacks, wallets, purses on such persons.



ATTACHMENT B-1

A. ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of Mail Fraud in violation of 18 U.S.C. § 1341, Wire Fraud in violation of 18 U.S.C. § 1343, Bank Fraud in violation of 18 U.S.C. § 1344, Aggravated Identity Theft in violation of 18 U.S.C. § 1028A and Conspiracy to Commit Wire Fraud and Bank Fraud in violation of 18 U.S.C. § 1349:

1. Records and other materials, including notes, ledgers, envelopes, and packaging materials, relating to solicitation and/or receipt of cash, money orders, checks, or wire transfers that were sent to Patrick JOHNSON, Patricia JOHNSON, to known and unknown conspirators, including but not limited to, Terrance Richardson, and Richard Koboi and to entities in the name of or associated with Patrick JOHNSON and/or Patricia JOHNSON;

Records and other materials, including notes, ledgers, envelopes, and packaging materials, relating to receipt of cash, money orders, counterfeit checks, or wire transfers that were involved in the fraud scheme;

2. Records relating to any communications by, between, and among Patrick JOHNSON and/or Patricia JOHNSON, victims, and known and unknown conspirators, including but not limited to, Terrance Richardson, and Richard Koboi relating to the receipt, solicitation, and transfer of funds and/or any counterfeit check cashing scheme;

3. Records relating to the means of identifications including, but not limited to name, social security number, date of birth of other individuals, banking account information of other individuals, and the use and/or creation of false identifications and personas;

4. Any and all opened or sealed USPS Priority or other mail envelopes and packages and receipts of the mailing transactions in relation to any counterfeit check scheme and/or the transfer and receipt of funds between the subjects of the investigation and other persons;

5. Records relating to the use, possession, and control of cellular telephones seized from the SUBJECT PREMISES 1 and/or any person located therein, and any landline telephones or internet service associated with the SUBJECT PREMISES 1;

6. Records relating to any communications with co-conspirators and victims, including telephone, electronic, or in person communications with co-conspirators and victims in relation to the specified federal offenses, any counterfeit checks, the transfer and receipt of funds between the subjects of the investigation and other persons;

7. Records, documents, and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry, or other items obtained with the proceeds from a fraud;

8. Documents and articles of personal property reflecting the identity of persons and/or entities occupying, possessing, residing in, owning, frequenting, or controlling the SUBJECT PREMISES 1, including keys, rental agreements and records, utility bills and receipts, photographs, answering machine tape recordings, telephone, vehicle records, canceled mail envelopes, correspondence, financial documents such as tax returns, bank records, safety deposit box records, canceled checks, and other records of income and expenditure, credit card records, travel documents, personal identification documents, including birth certificates, driver's license, immigration cards, and other forms of identification;

9. Any records which document an association with co-conspirators, including photographs, video and audio recordings;

10. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) in relation to a counterfeit check scheme and/or the transfer and receipt of funds between the subjects of the investigation and other persons;

11. Checks, ATM and bank deposit/withdrawal receipts, stock paper for producing counterfeit checks;

12. Banking, money remitter, and financial institution records, including but not limited to bank statements, credit card statements, canceled checks, money orders, deposit slips, orders for receipt or sending of money transfer by wire, checking and savings books, financial institution statements, records of safe deposit boxes, Whayee Sarkpah-Johnson's Citizens Bank debit card ending in 5301, and Patricia Johnson's Citizens Bank Account records including associated debit card ending in 0873;

13. Clothing worn by Patrick JOHNS ON while mailing out counterfeit checks including a black shirt with the word "STACKS" in white block lettering and a two-tone gray cardigan;

14. Handwritten documents associated with Patricia JOHNSON and Patrick JOHNSON;

15. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information whose seizure is authorized by this warrant, including any cell phones and printers (hereinafter, "COMPUTER"):

    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs,

registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
c. evidence of the lack of such malicious software;
d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;
f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
h. evidence of the times the COMPUTER was used;
i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
k. records of or information about Internet Protocol addresses used by the COMPUTER; and
l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMS, and other magnetic or optical media.

16. Routers, modems, and network equipment used to connect computers to the Internet.

17. As used in this Attachment, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

18. With respect to any and all electronically stored information in cellular telephones, in addition to the information described herein, agents may also access, record and seize the following:
    a. Telephone numbers of incoming/outgoing calls stored in the call registry;
    b. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
    c. Any incoming/outgoing text messages relating to the above criminal violations;
    d. Telephone subscriber information;
    e. The telephone numbers stored in the cellular telephone and/or PDA;
    f. records relating to the use, possession, and control of any cellular telephones seized;
    g. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular telephone including but not limited to photographs, videos, e-mail, and voice mail relating to the above criminal violations.

19. Contextual information necessary to understand the evidence described in this attachment.

II. AUTHORIZED SEARCH PROCEDURE

1. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

2. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:
    a. Any computer or storage medium capable of being used to commit further or store evidence of the Specified Federal Offenses; and
    b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

3. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.

B. <u>SEARCH PROCEDURE FOR DEVICES CAPABLE OF BIOMETRIC ACCESS</u>

1. During the execution of this search warrant, law enforcement is permitted to:

    a. depress PATRICK JOHNSON'S and/or PATRICIA JOHNSON's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and

b. hold the device in front of PATRICK JOHNSON and/or PATRICIA JOHNSON's face with her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

ATTACHMENT A-2

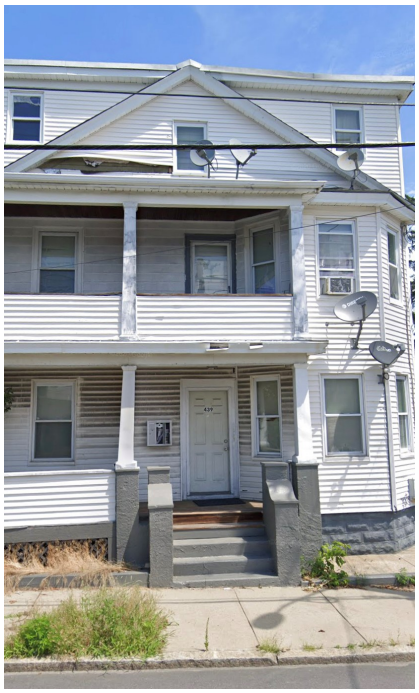
PREMISES TO BE SEARCHED

The SUBJECT PREMISES 2 is the premises at 439 Admiral Street, Apt 3, Providence, RI 02908. SUBJECT PREMISES 2 is described as a multi-family home. SUBJECT PREMISES 2 is a multi-family home directly across the street from Providence Fire Department Engine Co. 12 located at the corner of Dante Street and Admiral Street. The numbers "439" is clearly marked in black numbers on the front door.

The area to be searched at the SUBJECT PREMISES 2 includes all rooms, annexes, attics, basements, porches, garages, carports, outside yard area, curtilage, mailboxes, trash containers, debris boxes, storage lockers, locked containers and safes, lockers, sheds, and any visible structures and outbuildings associated with the SUBJECT PREMISES 2 and shall extend into desks, cabinets, safes, briefcases, backpacks, wallets, purses, digital devices, and any other storage locations within SUBJECT PREMISES 2.

The search shall also include any computers, cellular telephones, storage media/medium, and digital devices.

The search shall also include any person located at the SUBJECT PREMISES 2, as defined above, at the time the search warrant is executed, and any computers, cellular telephones, storage media/medium, briefcases, backpacks, wallets, purses on such persons.



ATTACHMENT B-2

A. ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of Bank Fraud in violation of 18 U.S.C. § 1344, Wire Fraud in violation of 18 U.S.C. § 1343, Conspiracy to Commit Wire and Bank Fraud in violation of 18 U.S.C. § 1349, Aggravated Identity Theft in violation of 18 U.S.C. §1028A, and Felon in Possession of a Firearm in violation of 21 U.S.C. 922(g)(1):

1. Records and other materials, including notes, ledgers, envelopes, and packaging materials, relating to solicitation and/or receipt of cash, money orders, checks, or wire transfers that were sent to Terrance RICHARDSON, to known and unknown conspirators, including but not limited to, Patrick Johnson, Patricia Johnson, and Richard Koboi, and to entities in the name of or associated with Terrance RICHARDSON'

Records and other materials, including notes, ledgers, envelopes, and packaging materials, relating to receipt of cash, money orders, counterfeit checks, or wire transfers that were involved in the fraud scheme;

2. Records relating to any communications by, between, and among Terrance RICHARDSON, victims, and known and unknown conspirators, including but not limited to, Patrick Johnson, Patricia Johnson, and Richard Koboi relating to the receipt, solicitation, and transfer of funds and/or any counterfeit check cashing scheme;

3. Records relating to the means of identifications including, but not limited to name, social security number, date of birth of other individuals, banking account information of other individuals, and the use and/or creation of false identifications and personas.

4. Any and all opened or sealed USPS Priority or other mail envelopes and packages and receipts of the mailing transactions in relation to any counterfeit check scheme and/or the transfer and receipt of funds between the subjects of the investigation and other persons;

5. Records relating to the use, possession, and control of cellular telephones seized from the SUBJECT PREMISES 2 and/or any person located therein, and any landline telephones or internet service associated with the SUBJECT PREMISES 2;

6. Records relating to any communications with co-conspirators and victims, including telephone, electronic, or in person communications with co-conspirators and victims in relation to the specified federal offenses, any counterfeit checks, the transfer and receipt of funds between the subjects of the investigation and other persons;

7. Records, documents, and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry, or other items obtained with the proceeds from a fraud;

8. Documents and articles of personal property reflecting the identity of persons and/or entities occupying, possessing, residing in, owning, frequenting, or controlling the SUBJECT PREMISES 2, including keys, rental agreements and records, utility bills and receipts, photographs, answering machine tape recordings, telephone, vehicle records, canceled mail envelopes, correspondence, financial documents such as tax returns, bank records, safety deposit box records, canceled checks, and other records of income and expenditure, credit card records, travel documents, personal identification documents, including birth certificates, driver's license, immigration cards, and other forms of identification;

9. Any records which document an association with co-conspirators, including photographs, video and audio recordings;

10. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) in relation to a counterfeit check scheme and/or the transfer and receipt of funds between the subjects of the investigation and other persons;

11. Checks, ATM deposit/withdrawal receipts, stock paper for producing counterfeit checks;

12. Banking, money remitter, and financial institution records, including but not limited to bank statements, credit card statements, canceled checks, money orders, deposit slips, orders for receipt or sending of money transfer by wire, checking and savings books, financial institution statements, records of safe deposit boxes, and debit cards in RICHARDSON's name and other people's names;

13. Clothing and jewelry worn by Terrance RICHARDSON while depositing counterfeit checks or withdrawing funds following the deposit of a counterfeit check including an orange shirt with black outline and a gold necklace and diamond pendant with the name "TEE BONE";

14. Firearms and ammunition, photographs of firearms and ammunition, and communications with respect to firearms and ammunition;

15. Handwritten documents associated with Terrance Richardson.

16. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored

records or information whose seizure is authorized by this warrant, including any cell phones and printers (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
c. evidence of the lack of such malicious software;
d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;
f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
h. evidence of the times the COMPUTER was used;
i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
k. records of or information about Internet Protocol addresses used by the COMPUTER; and
l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMS, and other magnetic or optical media.

17. Routers, modems, and network equipment used to connect computers to the Internet.

18. As used in this Attachment, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as

hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

19. With respect to any and all electronically stored information in cellular telephones, in addition to the information described herein, agents may also access, record and seize the following:
    a. Telephone numbers of incoming/outgoing calls stored in the call registry;
    b. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
    c. Any incoming/outgoing text messages relating to the above criminal violations;
    d. Telephone subscriber information;
    e. The telephone numbers stored in the cellular telephone and/or PDA;
    f. records relating to the use, possession, and control of any cellular telephones seized;
    g. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular telephone including but not limited to photographs, videos, e-mail, and voice mail relating to the above criminal violations.

20. Contextual information necessary to understand the evidence described in this attachment.

II. AUTHORIZED SEARCH PROCEDURE

1. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

2. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:
    a. Any computer or storage medium capable of being used to commit further or store evidence of the Specified Federal Offenses; and
    b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

3. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.

B. <u>SEARCH PROCEDURE FOR DEVICES CAPABLE OF BIOMETRIC ACCESS</u>

1. During the execution of this search warrant, law enforcement is permitted to:

a. depress the TERRANCE RICHARDSON's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and
b. hold the device in front of the TERRANCE RICHARDSON's face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

ATTACHMENT A-3

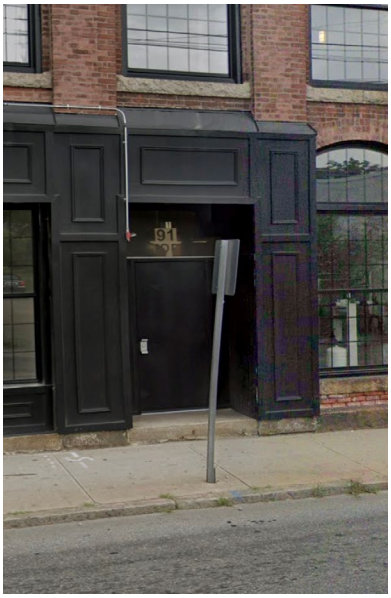
PREMISES TO BE SEARCHED

The SUBJECT PREMISES 3 is the premises at 91 Hartford Avenue, Apt 131, Providence, RI 02909. SUBJECT PREMISES 3 is described as multi-unit loft apartments. SUBJECT PREMISES 3 are multi-unit loft apartments directly across the street from Olneyville Post Office located on Hartford Avenue just prior to the Route 6 on-ramp. The numbers "91" is clearly marked in black numbers on the Hartford Ave entrance. The main entrance to the apartment building is in the rear parking lot on the adjacent side of the building.

The area to be searched at the SUBJECT PREMISES 3 includes all rooms, annexes, attics, basements, porches, garages, carports, outside yard area, curtilage, mailboxes, trash containers, debris boxes, storage lockers, locked containers and safes, lockers, sheds, and any visible structures and outbuildings associated with the SUBJECT PREMISES 3 and shall extend into desks, cabinets, safes, briefcases, backpacks, wallets, purses, digital devices, and any other storage locations within SUBJECT PREMISES 3.

The search shall also include any computers, cellular telephones, storage media/medium, and digital devices.

The search shall also include any person located at the SUBJECT PREMISES 3, as defined above, at the time the search warrant is executed, and any computers, cellular telephones, storage media/medium, briefcases, backpacks, wallets, purses on such persons.



ATTACHMENT B-3

A. ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of Bank Fraud in violation of 18 U.S.C. § 1344, Wire Fraud in violation of 18 U.S.C. § 1343, Conspiracy to Commit Wire and Bank Fraud in violation of 18 U.S.C. § 1349, Aggravated Identity Theft in violation of 18 U.S.C. §1028A, and Felon in Possession of a Firearm in violation of 21 U.S.C. 922(g)(1)::

1. Records and other materials, including notes, ledgers, envelopes, and packaging materials, relating to solicitation and/or receipt of cash, money orders, checks, or wire transfers that were sent to Richard KOBOI, to known and unknown conspirators, including but not limited to, Patrick Johnson, Patricia Johnson, and Terrance Richardson, and to entities in the name of or associated with Richard KOBOI.

2. Records and other materials, including notes, ledgers, envelopes, and packaging materials, relating to receipt of cash, money orders, counterfeit checks, or wire transfers that were involved in the fraud scheme;

3. Records relating to any communications by, between, and among Richard KOBOI, victims, and known and unknown conspirators, including but not limited to, Patrick Johnson, Patricia Johnson, and Terrance Richardson relating to the receipt, solicitation, and transfer of funds and/or any counterfeit check cashing scheme.

4. Records relating to the means of identifications including, but not limited to name, social security number, date of birth of other individuals, banking account information of other individuals, and the use and/or creation of false identifications and personas.

5. Any and all opened or sealed USPS Priority or other mail envelopes and packages and receipts of the mailing transactions, in relation to any counterfeit check scheme and/or the transfer and receipt of funds between the subjects of the investigation and other persons;

6. Records relating to the use, possession, and control of cellular telephones seized from the SUBJECT PREMISES 3 and/or any person located therein, and any landline telephones or internet service associated with the SUBJECT PREMISES 3;

7. Records relating to any communications with co-conspirators and victims, including telephone, electronic, or in person communications with co-conspirators and victims in relation to the specified federal offenses, any counterfeit checks, the transfer and receipt of funds between the subjects of the investigation and other persons;

8. Records, documents, and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry, or other items obtained with the proceeds from a fraud;

9. Documents and articles of personal property reflecting the identity of persons and/or entities occupying, possessing, residing in, owning, frequenting, or controlling the SUBJECT PREMISES 3, including keys, rental agreements and records, utility bills and receipts, photographs, answering machine tape recordings, telephone, vehicle records, canceled mail envelopes, correspondence, financial documents such as tax returns, bank records, safety deposit box records, canceled checks, and other records of income and expenditure, credit card records, travel documents, personal identification documents, including birth certificates, driver's license, immigration cards, and other forms of identification;

10. Any records which document an association with co-conspirators, including photographs, video and audio recordings;

11. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) in relation to a counterfeit check scheme and/or the transfer and receipt of funds between the subjects of the investigation and other persons;

12. Checks, ATM deposit/withdrawal receipts, stock paper for producing counterfeit checks;

13. Banking, money remitter, and financial institution records, including but not limited to bank statements, credit card statements, canceled checks, money orders, deposit slips, orders for receipt or sending of money transfer by wire, checking and savings books, financial institution statements, records of safe deposit boxes, and debit cards in KOBOI's and other people's names;

14. Clothing and jewelry worn by Richard KOBOI while depositing counterfeit checks or withdrawing funds following the deposit of a counterfeit check including an yellow sweatshirt with the word "passion" written in black lettering on the front and two gold necklaces, one with a padlock shaped pendant and the other a rectangle shaped pendant.

15. Firearms and ammunition, photographs of firearms and ammunition, and communications with respect to firearms and ammunition;

16. Handwritten documents associated with Richard KOBOI.

17. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information whose seizure is authorized by this warrant, including any cell phones (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
c. evidence of the lack of such malicious software;
d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;
f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
h. evidence of the times the COMPUTER was used;
i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
k. records of or information about Internet Protocol addresses used by the COMPUTER; and
l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMS, and other magnetic or optical media.

18. Routers, modems, and network equipment used to connect computers to the Internet.

19. As used in this Attachment, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

20. With respect to any and all electronically stored information in cellular telephones, in addition to the information described herein, agents may also access, record and seize the following:
    a. Telephone numbers of incoming/outgoing calls stored in the call registry;
    b. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
    c. Any incoming/outgoing text messages relating to the above criminal violations;
    d. Telephone subscriber information;
    e. The telephone numbers stored in the cellular telephone and/or PDA;
    f. records relating to the use, possession, and control of any cellular telephones seized;
    g. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular telephone including but not limited to photographs, videos, e-mail, and voice mail relating to the above criminal violations.

21. Contextual information necessary to understand the evidence described in this attachment.

II. AUTHORIZED SEARCH PROCEDURE

1. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

2. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:
    a. Any computer or storage medium capable of being used to commit further or store evidence of the Specified Federal Offenses; and
    b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

3. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.

B. SEARCH PROCEDURE FOR DEVICES CAPABLE OF BIOMETRIC ACCESS

1. During the execution of this search warrant, law enforcement is permitted to:

   a. depress RICHARD KOBOI's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and
   b. hold the device in front of RICHARD KOBOI's face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

ATTACHMENT C-1

Property to Be Searched

The cellular telephone assigned call number (401) 677-9165, IMSI: 310260270097507 ("TARGET PHONE #1"), whose wireless service provider is T -Mobile, a company located out of Parsippany, New Jersey.

Information about the location of TARGET PHONE #1 that is within the possession, custody, or control of T -Mobile, including information about the location of the cellular telephone if it is subsequently assigned a different call number.

ATTACHMENT C-2

Property to Be Searched

The cellular telephone assigned call number (267) 854-9972, ("TARGET PHONE #2) whose wireless service provider is T -Mobile, a company located out of Parsippany, New Jersey.

Information about the location of TARGET PHONE #2 that is within the possession, custody, or control of T -Mobile, including information about the location of the cellular telephone if it is subsequently assigned a different call number.

ATTACHMENT D

Particular Things to be Seized

I. Information to be Disclosed by the Provider

All information about the location of the TARGET PHONES #1 and #2 described in Attachment A-1 and A-2 for a period of thirty days, during all times of day and night. "Information about the location of the TARGET PHONES" includes all available E-911 Phase II data, GPS data, latitude- longitude data, and other precise location information, as well as all data about which "cell towers" (i.e., antenna towers covering specific geographic areas) and "sectors" (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of T-Mobile, T-Mobile is required to disclose the Location Information to the government. In addition, T-Mobile must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with T-Mobile's services, including by initiating a signal to determine the location of the TARGET PHONES on T-Mobile network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate T-Mobile for reasonable expenses incurred in furnishing such facilities or assistance.

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a (b).

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 1344 (Bank Fraud),18 U.S.C. § 1349 (Conspiracy to Commit Bank Fraud), and 18 U.S.C. § 1028A (Aggravated Identity Theft) involving Terrance RICHARDSON, Richard KOBOI and others.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.